



Guía del usuario

Incident Manager



Incident Manager: Guía del usuario

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Systems Manager Incident Manager?	1
Componentes y características principales	1
Beneficios del uso de Incident Manager	3
Servicios relacionados	5
Acceso a Incident Manager	5
Regiones y cuotas de Incident Manager	5
Precios de Incident Manager	6
Ciclo de vida de los incidentes	6
Alerta e intervención	7
Triaje	8
Investigación y mitigación	9
Análisis post-incidente	10
Configuración	12
Regístrese para obtener una Cuenta de AWS	12
Creación de un usuario con acceso administrativo	13
Conceder acceso programático	14
Rol requerido para la configuración de Incident Manager	16
Introducción	17
Requisitos previos	17
Asistente de preparación	17
Administración de incidentes entre regiones y entre cuentas	24
Administración de incidentes entre regiones	24
Administración de incidentes entre cuentas	25
Prácticas recomendadas	25
Instalación y configuración de la administración de incidentes entre cuentas	26
Limitaciones	28
Preparación para incidentes	29
Supervisión	31
Uso de los ajustes generales	32
Conjunto de réplica	32
Administración de las etiquetas de un conjunto de réplica	33
Administración de la característica Resultados	34
Uso de contactos	35
Canales de contacto	35

Planes de participación	37
Creación de un contacto	37
Importación de datos de contacto a su libreta de direcciones	38
Uso de los horarios de guardia	38
Creación de un horario de guardia	39
Administración de un horario de guardia existente	44
Uso de los planes de escalada	50
Escenarios	50
Creación de un plan de escalada	51
Uso de los canales de chat	51
Tarea 1: Crear o actualizar temas de Amazon SNS para su canal de chat	52
Tarea 2: Crear un canal de chat en AWS Chatbot	54
Tarea 3: Añadir el canal de chat a un plan de respuesta en Incident Manager	57
Interacción a través del canal de chat	57
Uso de manuales de procedimientos	58
Permisos de IAM necesarios para iniciar y ejecutar flujos de trabajo de manuales de procedimientos	59
Uso de los parámetros del manual de procedimientos	62
Definición de un manual de procedimientos	64
Plantilla de manual de procedimientos de Incident Manager	65
Uso de los planes de respuesta	67
Creación de un plan de respuesta	68
Uso de los resultados	75
Habilitación y creación de un rol de servicio de resultados	76
Configuración de permisos para el soporte de resultados entre cuentas	76
Creación de incidentes	77
Creación automática de incidentes con alarmas de CloudWatch	78
Creación automática de incidentes con eventos de EventBridge	79
Creación de incidentes mediante eventos de socios SaaS	79
Creación de incidentes mediante eventos de servicios de AWS	81
Creación manual de incidentes	82
Seguimiento de incidentes	83
Lista de incidentes	83
Detalles del incidente	83
Banner superior	84
Notas del incidente	85

Pestañas	85
Información general	86
Diagnóstico	86
Plazo	88
Manuales de procedimientos	88
Participaciones	89
Elementos relacionados	90
Propiedades	90
Realización de un análisis post-incidente	92
Detalles del análisis	92
Información general	92
Métricas	93
Plazo	93
Preguntas	94
Acciones	94
Lista de comprobación	94
Plantillas de análisis	95
Plantillas estándar de AWS	95
Creación de una plantilla de análisis	95
Creación de un análisis	96
Impresión de un análisis de incidente formateado	96
Tutoriales	98
Uso de los manuales de procedimientos con Administración de incidentes	98
Tarea 1: Creación del manual de procedimientos	99
Tarea 2: Creación de un rol de IAM	102
Tarea 3: Conexión del manual de procedimientos a su plan de respuesta	104
Tarea 4: Asignar una CloudWatch alarma a su plan de respuesta	105
Tarea 5: Verificación de resultados	106
Administración de incidentes de seguridad	107
Etiquetado de recursos	109
Seguridad	111
Protección de datos	112
Cifrado de datos	113
Identity and Access Management	115
Público	115
Autenticación con identidades	116

Administración de acceso mediante políticas	120
¿Cómo AWS Systems Manager Incident Manager funciona con IAM	122
Ejemplos de políticas basadas en identidades	130
Ejemplos de políticas basadas en recursos	135
Prevención de la sustitución confusa entre servicios	137
Uso de roles vinculados a servicios	138
AWS políticas gestionadas para Incident Manager	141
Resolución de problemas	148
Uso compartido de contactos y planes de respuesta en Incident Manager	150
Requisitos previos para compartir contactos y planes de respuesta	151
Servicios relacionados	151
Uso compartido de un contacto o un plan de respuesta	152
Detención del uso compartido de un contacto o un plan de respuesta	152
Identificación de un contacto o plan de respuesta compartidos	153
Permisos de los contactos y planes de respuesta compartidos	154
Facturación y medición	154
Límites de instancias	154
Validación de conformidad	154
Resiliencia	156
Seguridad de la infraestructura	156
Trabajar con VPC puntos finales ()AWS PrivateLink	157
Consideraciones sobre los puntos finales de Incident Manager VPC	157
Crear un VPC punto final de interfaz para Incident Manager	158
Creación de una política VPC de puntos finales para Incident Manager	158
Configuración y análisis de vulnerabilidades	159
Prácticas recomendadas de seguridad	159
Prácticas recomendadas de seguridad preventivas para Incident Manager	159
Las mejores prácticas recomendadas de seguridad de detección para Incident Manager	161
Supervisión	163
CloudWatch Métricas de Amazon en Incident Manager	163
Visualización de las métricas de Incident Manager en la CloudWatch consola	166
Dimensiones de métricas	166
Registro de llamadas a la AWS Systems Manager Incident Manager API mediante AWS	
CloudTrail	167
Eventos de gestión de incidentes de Incident Manager en CloudTrail	169
Ejemplos de eventos de Incident Manager	169

Integraciones de productos y servicios	172
Integración con Servicios de AWS	172
Integración a otros productos y servicios	177
Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager	183
Solución de problemas	189
Mensaje de error: ValidationException - We were unable to validate the AWS Secrets Manager secret	189
Otras incidencias en la solución de problemas	191
Glosario de AWS	192
Historial de documentos	193
.....	ccxi

¿Qué es AWS Systems Manager Incident Manager?

Incident Manager, una capacidad de AWS Systems Manager, está diseñado para ayudarle a mitigar incidentes que afecten a sus aplicaciones alojadas en AWS y a recuperarse de los mismos.

En el contexto de AWS, un incidente es cualquier interrupción no planificada o reducción de calidad de los servicios que pueda tener un impacto significativo en las operaciones empresariales. Por lo tanto, es esencial que las organizaciones establezcan una estrategia de respuesta de mitigación y recuperación eficaz ante incidentes e implementen acciones para prevenirlos en el futuro.

Para ayudar a reducir el tiempo de resolución de incidentes, Incident Manager:

- Proporciona planes automatizados que involucra de manera eficiente a las personas responsables de responder a los incidentes.
- Proporciona datos relevantes para la solución de problemas.
- Habilita acciones de respuesta automatizadas mediante manuales de procedimientos de automatización predefinidos.
- Proporciona métodos para colaborar y comunicar con todas las partes interesadas.

Las características y los flujos de trabajo integrados en Incident Manager se basan en las prácticas recomendadas de respuesta a incidentes que Amazon ha venido desarrollando casi desde su creación. Incident Manager se integra con Servicios de AWS como Amazon CloudWatch, AWS CloudTrail, AWS Systems Manager y Amazon EventBridge.

Componentes y características principales

En esta sección se describen las características de Incident Manager que usted utiliza para configurar sus planes de respuesta a incidentes.

Plan de respuesta

Un plan de respuesta funciona como una plantilla que define lo que se debe establecer al producirse un incidente. Incluye información como:

- Quién debe responder al producirse un incidente.
- La respuesta automatizada establecida para mitigar el incidente.

- La herramienta de colaboración que los respondedores deben utilizar para comunicar y recibir notificaciones automáticas sobre el incidente.

Detección de incidentes

Puede configurar alarmas de Amazon CloudWatch y eventos de Amazon EventBridge para crear incidentes al detectarse condiciones o cambios que afecten a sus recursos de AWS.

Soporte de automatización de manuales de procedimientos

Puede iniciar manuales de procedimientos de automatización desde Incident Manager para automatizar su respuesta crítica a los incidentes y proporcionar pasos detallados a los respondedores iniciales.

Participación y escalada

Un plan de participación especifica a quiénes se debe enviar una notificación para cada incidente único. Puede especificar contactos individuales que haya añadido a Incident Manager o especificar un horario de guardia que haya creado en Incident Manager. Los planes de participación también especifican una ruta de escalada para ayudar a garantizar la visibilidad entre las partes interesadas y la participación activa durante el proceso de respuesta a incidentes.

Horarios de guardia

Un horario de guardia en Incident Manager consta de una o más rotaciones que usted crea para el horario. Para cada rotación, puede incluir hasta 30 contactos. El horario de guardia, al añadirlo a un plan de escalada o de respuesta, define a quién se notifica al producirse un incidente que requiera la intervención de un respondedor. Los horarios de guardia le permiten asegurarse de que dispone de una cobertura completa, redundante e ininterrumpida (24/7) según sea necesario para su respuesta a incidentes.

Colaboración activa

Los respondedores de incidentes responden activamente a los incidentes a través de la integración con el cliente de AWS Chatbot. AWS Chatbot admite la creación de canales de chat para Incident Manager que utilicen Slack, Microsoft Teams o Amazon Chime. Los respondedores pueden comunicar directamente entre sí, recibir notificaciones automáticas sobre incidentes y, en Slack y Microsoft Teams, ejecutar directamente algunas operaciones de la interfaz de la línea de comandos (CLI) de Incident Manager.

Diagnóstico de incidentes

Los respondedores pueden ver información actualizada en la consola de Incident Manager durante un incidente. En función de los cambios en la información, los respondedores pueden

crear elementos de seguimiento y corregirlos mediante manuales de procedimientos de automatización.

Resultados de otros servicios

Para apoyar el diagnóstico de incidentes de los respondedores, puede habilitar la característica Resultados en Incident Manager. Los resultados son información sobre implementaciones de AWS CodeDeploy y actualizaciones de la pila de AWS CloudFormation que se produjeron alrededor del momento de un incidente y que implicaron a uno o más recursos probablemente relacionados con el incidente. Disponer de esta información reduce el tiempo necesario para evaluar las causas potenciales, lo que puede reducir el tiempo medio de recuperación (MTTR) de un incidente.

Análisis post-incidente

Una vez resuelto un incidente, utilice un análisis post-incidente para identificar mejoras en su respuesta a incidentes, incluyendo el tiempo de detección y mitigación. Un análisis también puede ayudarle a comprender la causa raíz de los incidentes. Incident Manager crea elementos de acción de seguimiento recomendados que puede utilizar para mejorar su respuesta a los incidentes.

Beneficios del uso de Incident Manager

Obtenga información sobre los beneficios que brinda Incident Manager en sus operaciones de detección y respuesta a incidentes.

En esta sección se describen los beneficios que su organización puede obtener al implementar un plan de respuesta con Incident Manager.

Diagnóstico de problemas de manera eficaz e inmediata

Las alarmas de Amazon CloudWatch y los eventos de Amazon EventBridge que configure pueden crear incidentes automáticamente al producirse cualquier interrupción imprevista o reducción de calidad de sus servicios.

Las alarmas de CloudWatch detectan e informan al producirse cambios en el valor de la métrica o expresión en relación con un umbral a lo largo de una serie de periodos de tiempo. Los eventos de EventBridge se crean como resultado de un cambio en un entorno, aplicación o servicio que haya especificado en una regla de EventBridge. Al crear una alarma o un evento, puede especificar una

acción para que se cree un incidente en Incident Manager y el plan de respuesta apropiado para facilitar el afrontamiento, la escalada y la mitigación del incidente.

Incident Manager ofrece la posibilidad de recopilar y realizar un seguimiento automático de las métricas relacionadas con un incidente, mediante el uso de las métricas de CloudWatch. Además de las métricas automatizadas generadas para el incidente que este crea a través de una alarma de CloudWatch, puede añadir métricas manualmente en tiempo real a fin de proporcionar contexto y datos adicionales a los respondedores en un incidente.

Utilice la línea temporal de incidentes de Incident Manager para mostrar los puntos de interés en orden cronológico. Los respondedores también pueden utilizar la línea temporal para añadir eventos personalizados que describan lo que hicieron o lo que ocurrió. Los puntos de interés automatizados incluyen:

- Una alarma de CloudWatch o una regla de EventBridge crea un incidente.
- Las métricas de los incidentes se comunican a Incident Manager.
- Los respondedores participan.
- Los pasos del manual de procedimientos se completan con éxito.

Participación eficaz

Incident Manager reúne a los respondedores de incidentes mediante el uso de contactos, horarios de guardia, planes de escalada y canales de chat. Usted define los contactos individuales directamente en Incident Manager y especifica las preferencias de contacto (correo electrónico, SMS o voz). Usted añade contactos a las rotaciones de los planes de guardia para determinar quién está encargado de atender las incidencias durante un periodo determinado. Al utilizar los contactos definidos y los horarios de guardia, usted crea planes de escalada para involucrar a los respondedores necesarios en el momento adecuado durante un incidente.

Colaboración en tiempo real

La comunicación durante un incidente es el elemento clave para una resolución más rápida. Mediante un cliente de AWS Chatbot configurado para utilizar Slack, Microsoft Teams o Amazon Chime, puede reunir a los respondedores en su canal de chat conectado preferido, donde interactúan directamente con el incidente y entre sí. Incident Manager también muestra las acciones en tiempo real de los respondedores de incidentes en el canal de chat, proporcionando contexto a los demás.

Automatización del restablecimiento del servicio

Incident Manager permite a sus respondedores centrarse en las tareas clave necesarias para resolver un incidente mediante el uso de manuales de procedimientos automatizados. En Incident Manager, los manuales de procedimientos son una serie de acciones predefinidas para resolver un incidente. Combinan la potencia de las tareas automatizadas con pasos manuales según sea necesario, lo que da a los respondedores más disponibilidad para analizar y responder al impacto.

Prevención de futuros incidentes

Mediante el análisis post-incidente de Incident Manager, su equipo puede desarrollar planes de respuesta más sólidos y efectuar cambios en todas sus aplicaciones para prevenir futuros incidentes y tiempos de inactividad. El análisis post-incidente también permite el aprendizaje iterativo y la mejora de los manuales de procedimientos, los planes de respuesta y las métricas.

Servicios relacionados

Incident Manager se integra con varios otros Servicios de AWS y servicios de terceros y herramientas para ayudarle a detectar y resolver incidentes, y para interactuar con sus operaciones de la API de forma indirecta y administrar la infraestructura. Para obtener información, consulte [Integraciones de productos y servicios con Incident Manager](#).

Acceso a Incident Manager

Puede acceder a Incident Manager de cualquiera de las siguientes formas:

- La [consola de Incident Manager](#)
- AWS CLI: Para obtener información general, consulte [Introducción a la AWS CLI](#) en la Guía del usuario de AWS Command Line Interface. Para obtener información sobre los comandos de la CLI de Incident Manager, consulte [ssm-incidents](#) y [ssm-contacts](#) en la Referencia de comandos de la AWS CLI.
- API de Incident Manager: Para obtener más información, consulte la [Referencia de la API de AWS Systems Manager Incident Manager](#).
- SDK de AWS: Para obtener más información, consulte [Herramientas para crear en AWS](#).

Regiones y cuotas de Incident Manager

Incident Manager no es compatible en todas las Regiones de AWS admitidas por Systems Manager.

Para obtener información sobre regiones y cuotas de Incident Manager, consulte [Puntos de conexión y cuotas de AWS Systems Manager Incident Manager](#) en Referencia general de Amazon Web Services.

Precios de Incident Manager

El uso de Incident Manager tiene un costo. Para obtener más información, consulte [Precios de AWS Systems Manager](#).

Note

Otros Servicios de AWS, contenidos de AWS y contenidos de terceros puestos a disposición en relación con este servicio podrían estar sujetos a cargos por separado y regirse por términos adicionales.

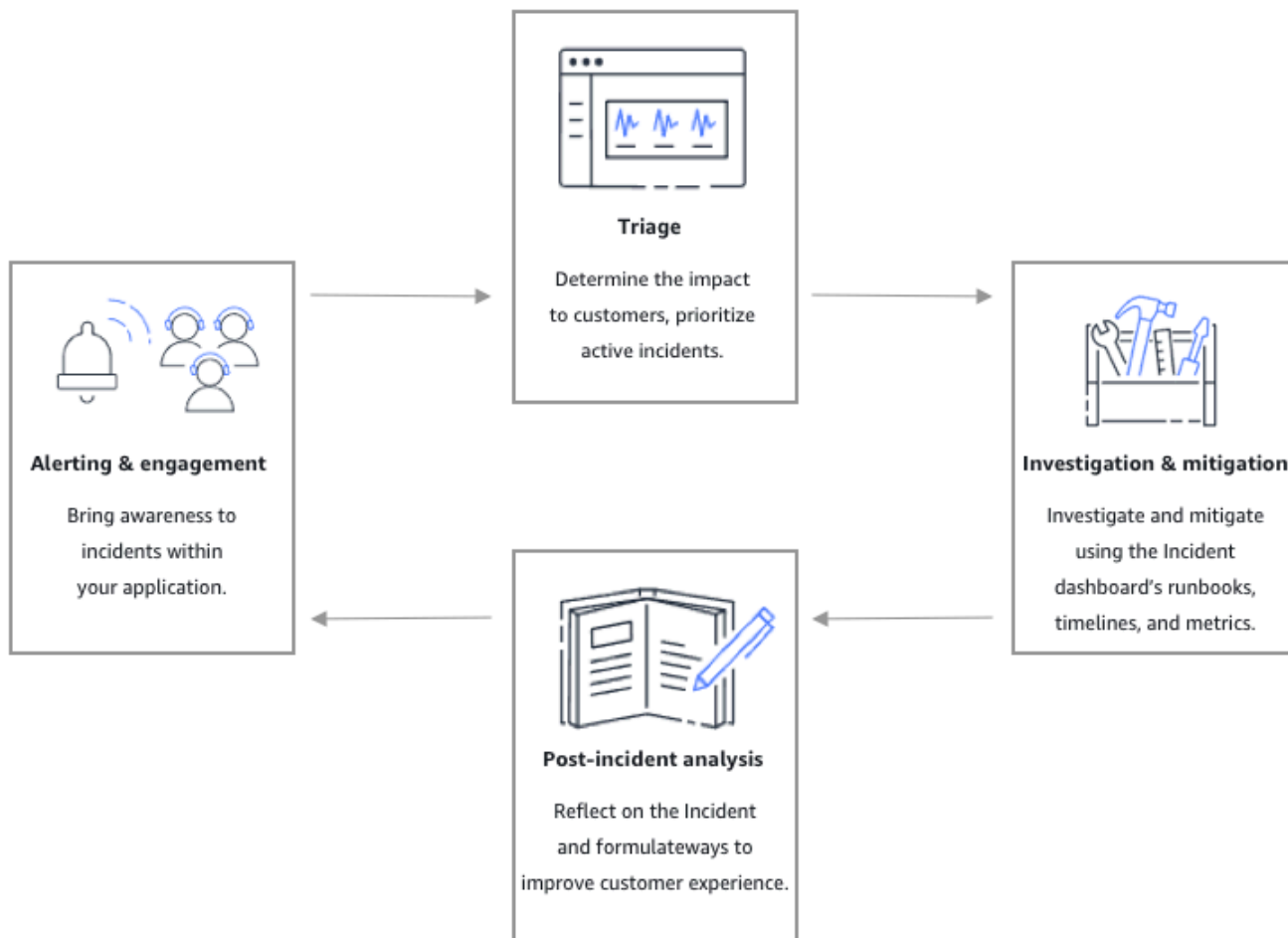
Para obtener una descripción general de Trusted Advisor, un servicio que le ayuda a optimizar los costos, la seguridad y el rendimiento de su entorno de AWS, consulte [AWS Trusted Advisor](#) en la Guía del usuario de AWS Support.

Ciclo de vida de los incidentes en Incident Manager

AWS Systems Manager Incident Manager proporciona un marco paso a paso basado en las prácticas recomendadas para identificar y reaccionar ante incidentes, como cortes de servicio o amenazas a la seguridad. El objetivo principal de Incident Manager es ayudar a restablecer la normalidad de los servicios o aplicaciones afectados lo antes posible mediante una solución completa de administración del ciclo de vida de los incidentes.

Incident Manager proporciona herramientas y prácticas recomendadas para cada fase del ciclo de vida de los incidentes:

- [Alerta e intervención](#)
- [Triage](#)
- [Investigación y mitigación](#)
- [Análisis post-incidente](#)



Alerta e intervención

La fase de alerta e intervención del ciclo de vida del incidente se centra en dar a conocer los incidentes dentro de sus aplicaciones y servicios. Esta fase comienza antes de que se detecte un incidente y requiere un profundo conocimiento de sus aplicaciones. Puede utilizar las [Métricas de Amazon CloudWatch](#) para monitorear datos sobre el rendimiento de sus aplicaciones, o aprovechar [Amazon EventBridge](#) para agregar alertas de diferentes orígenes, aplicaciones y servicios. Después de haber configurado el monitoreo de sus aplicaciones, puede comenzar a alertar sobre las métricas que se desvían de la norma histórica. Para obtener más información sobre las prácticas recomendadas de monitoreo, consulte [Supervisión](#).

Para apoyar el diagnóstico de incidentes de los respondedores, puede habilitar la característica Resultados en Incident Manager. Los resultados son información sobre implementaciones de AWS CodeDeploy y actualizaciones de la pila de AWS CloudFormation que se produjeron alrededor del

momento de un incidente. Disponer de esta información reduce el tiempo necesario para evaluar las causas potenciales, lo que puede reducir el tiempo medio de recuperación (MTTR) de un incidente.

Ahora que está monitoreando los incidentes en sus aplicaciones, puede definir un plan de respuesta a incidentes a fin de utilizarlo durante un incidente. Para obtener más información sobre la creación de planes de respuesta, consulte [Uso de los planes de respuesta en Incident Manager](#). Los eventos de Amazon EventBridge o las alarmas de CloudWatch pueden crear automáticamente un incidente utilizando como plantilla los planes de respuesta. Para obtener más información sobre la creación de incidentes, consulte [Creación de incidentes en Incident Manager](#).

Los planes de respuesta lanzan planes de escalada y planes de participación relacionados para atraer a los primeros respondedores al incidente. Para obtener más información sobre la creación de planes de escalada, consulte [Creación de un plan de escalada](#). Simultáneamente, AWS Chatbot notifica a los respondedores mediante un canal de chat, dirigiéndoles a la página de detalles del incidente. Mediante el canal de chat y los detalles del incidente, el equipo puede comunicar y clasificar un incidente. Para obtener más información sobre la configuración de canales de chat en Incident Manager, consulte [Tarea 2: Crear un canal de chat en AWS Chatbot](#).

Triaje

El triaje es cuando los primeros respondedores intentan determinar el impacto para los clientes. La vista de detalles del incidente en la consola de Incident Manager proporciona a los respondedores líneas temporales y métricas para ayudarles a evaluar el incidente. La evaluación del impacto de un incidente también sienta las bases para el tiempo de respuesta, la resolución y la comunicación del incidente. Los respondedores priorizan los incidentes utilizando clasificaciones de impacto del 1 (Crítico) al 5 (Sin impacto).

Su organización puede definir el alcance exacto de cada clasificación de impacto como prefiera. En la tabla siguiente se ofrecen ejemplos de cómo podría definirse normalmente cada nivel de impacto.

Código del impacto	Nombre del impacto	Ejemplo de alcance definido
1	Critical	Fallo total de una aplicación que repercute en la mayoría de los clientes.
2	High	Fallo total de una aplicación que repercute en un subconjunto de clientes.

Código del impacto	Nombre del impacto	Ejemplo de alcance definido
3	Medium	Fallo parcial de una aplicación que repercute en los clientes.
4	Low	Fallos intermitentes que tienen un impacto limitado en los clientes.
5	No Impact	Los clientes no se ven actualmente afectados, pero es necesario tomar medidas urgentes para evitar el impacto.

Investigación y mitigación

La vista de detalles del incidente proporciona a su equipo manuales de procedimientos, líneas temporales y métricas. Para obtener información sobre cómo puede trabajar con un incidente, consulte [Detalles del incidente](#).

Los manuales de procedimientos suelen proporcionar pasos de investigación y pueden extraer datos o intentar soluciones de uso común de forma automática. Los manuales de procedimientos también proporcionan pasos claros y repetibles que su equipo ha encontrado útiles para mitigar incidentes. La pestaña “Manual de procedimientos” se centra en el paso actual del manual de procedimientos y muestra los pasos pasados y futuros.

Incident Manager se integra con Systems Manager Automation para crear manuales de procedimientos. Utilice los manuales de procedimientos para realizar cualquiera de las siguientes acciones:

- Administrar instancias y recursos de AWS
- Ejecutar scripts de forma automática
- Administrar recursos de AWS CloudFormation

Para obtener más información sobre los tipos de acciones admitidos, consulte [Referencia de acciones de Systems Manager Automation](#) en la Guía del usuario de AWS Systems Manager.

La pestaña Línea temporal muestra las acciones que se han realizado. La línea temporal registra cada acción con una marca de tiempo y detalles creados automáticamente. Para añadir eventos personalizados a la línea temporal, consulte la sección [Plazo](#) en la página Detalles del incidente de esta guía del usuario.

La pestaña Diagnóstico muestra métricas introducidas tanto de forma automática como manual. Esta vista proporciona información valiosa sobre las actividades de su aplicación durante un incidente.

La pestaña Participaciones le permite añadir contactos adicionales al incidente y ayuda a proporcionar los recursos para que el contacto implicado se ponga al día rápidamente una vez involucrado en el incidente. Los contactos se comprometen a través de planes de escalada o planes de participación personal definidos.

Mediante un canal de chat, puede interactuar directamente con su incidente y con otros respondedores de su equipo. Mediante AWS Chatbot, puede configurar canales de chat en Slack, Microsoft Teams y Amazon Chime. En los canales Slack y Microsoft Teams, los respondedores pueden interactuar con los incidentes directamente desde el canal de chat utilizando una serie de comandos `ssm-incidents`. Para obtener más información, consulte [Interacción a través del canal de chat](#).

Análisis post-incidente

Incident Manager proporciona un marco para reflexionar sobre un incidente, tomar las medidas necesarias para evitar que se repita en el futuro y mejorar las actividades de respuesta a incidentes en general. Las mejoras pueden incluir:

- Cambios en las aplicaciones implicadas en un incidente. Su equipo puede utilizar este tiempo para mejorar el sistema y hacerlo más tolerante a los fallos.
- Cambios en un plan de respuesta a incidentes. Tómese el tiempo necesario para incorporar las lecciones aprendidas.
- Cambios en los manuales de procedimientos. Su equipo puede profundizar en los pasos necesarios para la resolución y en los pasos que usted puede automatizar.
- Cambios en las alertas. Tras un incidente, su equipo podría haber observado puntos críticos en las métricas que puede utilizar para alertar con antelación al equipo sobre un incidente.

Incident Manager facilita estas mejoras potenciales a través de un conjunto de preguntas de análisis post-incidente y elementos de acción junto con la línea temporal del incidente. Para obtener más

información sobre la mejora a través del análisis, consulte [Realización de un análisis post-incidente en Incident Manager](#).

Configuración de AWS Systems Manager Incident Manager

Recomendamos configurar AWS Systems Manager Incident Manager en la cuenta que utilice para gestionar sus operaciones. Antes de utilizar Incident Manager por primera vez, complete las siguientes tareas:

Temas

- [Regístrese para obtener una Cuenta de AWS](#)
- [Creación de un usuario con acceso administrativo](#)
- [Conceder acceso programático](#)
- [Rol requerido para la configuración de Incident Manager](#)

Regístrese para obtener una Cuenta de AWS

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWS se crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar [tareas que requieren acceso de usuario raíz](#).

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en <https://aws.amazon.com/> y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [AWS Management Console](#) como propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Signing in as the root user](#) en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz \(consola\)](#) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte [Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la](#) Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte [Create a permission set](#) en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

Conceder acceso programático

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a AWS Management Console. La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS CLI, AWS SDK o las API. AWS	<p>Siga las instrucciones de la interfaz que desea utilizar:</p> <ul style="list-style-type: none"> • Para ello AWS CLI, consulte Configuración del uso AWS IAM Identity Center en AWS CLI la Guía del AWS Command Line Interface usuario. • Para ver AWS los SDK, las herramientas y las AWS API, consulte la autenticación del IAM Identity Center en la Guía de referenci

¿Qué usuario necesita acceso programático?	Para	Mediante
		a de AWS los SDK y las herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: <ul style="list-style-type: none"> • Para ello AWS CLI, consulte Autenticación con credenciales de usuario de IAM en la Guía del usuario.AWS Command Line Interface • Para obtener información AWS sobre los SDK y las herramientas, consulte Autenticarse con credenciales de larga duración en la Guía de referencia de los AWS SDK y las herramientas. • Para obtener información AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Rol requerido para la configuración de Incident Manager

Antes de empezar, su cuenta debe tener el permiso IAM `iam:CreateServiceLinkedRole`. Incident Manager utiliza este permiso para crear el `AWSServiceRoleforIncidentManager` en su cuenta. Para obtener más información, consulte [Uso de roles vinculados a servicios para Incident Manager](#).

Introducción a Incident Manager

En esta sección se explica el asistente Preparación en la consola de Incident Manager. Deberá completar Preparación en la consola antes de poder utilizarla para la administración de incidentes. El asistente le guiará a través de la configuración del conjunto de réplica, al menos un contacto y un plan de escalada, y su plan de primera respuesta. Las siguientes guías le ayudarán a comprender Incident Manager y el ciclo de vida de los incidentes:

- [¿Qué es AWS Systems Manager Incident Manager?](#)
- [Ciclo de vida de los incidentes en Incident Manager](#)

Requisitos previos

Si es la primera vez que utiliza Incident Manager, consulte la [Configuración de AWS Systems Manager Incident Manager](#). Le recomendamos que configure Incident Manager en la cuenta que utilice para administrar sus operaciones.

Le recomendamos que complete la configuración rápida de Systems Manager antes de iniciar el asistente Preparación de Incident Manager. Utilice [Configuración rápida](#) de Systems Manager para configurar los servicios y características de AWS de uso frecuente con las prácticas recomendadas. Incident Manager utiliza las características de Systems Manager para administrar los incidentes asociados a su Cuentas de AWS y se beneficia de tener Systems Manager configurado en primer lugar.

Asistente de preparación

La primera vez que utilice Incident Manager, puede acceder al asistente Preparación desde la página de inicio del servicio Incident Manager. Para acceder al asistente Preparación después de completar la configuración inicial, elija Preparación en la página de la lista de Incidentes.


1. Abra la [consola de Incident Manager](#).
2. En la página de inicio del servicio Incident Manager, elija Preparación.

Configuración general

1. En Configuración general, elija Preparación.

2. Lea los términos y condiciones. Si acepta los términos y condiciones de Incident Manager, seleccione He leído y acepto los términos y condiciones de Incident Manager y, a continuación, elija Siguiente.
3. En el área Regiones, su Región de AWS actual aparece como la primera región de su conjunto de réplica. Para añadir más regiones a su conjunto de réplica, elíjalas en la lista de regiones.

Le recomendamos que incluya al menos dos regiones. En caso de que una región no esté disponible temporalmente, las actividades relacionadas con incidentes pueden seguir dirigiéndose a la otra región.

 Note

Al crear el conjunto de réplica se crea el rol vinculado al servicio `AWSServiceRoleforIncidentManager` en su cuenta. Para obtener más información sobre este rol, consulte [Uso de roles vinculados a servicios para Incident Manager](#).

4. Para configurar el cifrado de su conjunto de réplica, realice una de las siguientes acciones:

 Note

Todos los recursos de Incident Manager están cifrados. Para obtener más información sobre cómo se cifran sus datos, consulte [Protección de los datos en Incident Manager](#). Para obtener más información sobre su conjunto de réplica de Incident Manager, consulte [Uso del conjunto de réplica de Incident Manager](#).

- Para utilizar una clave propiedad de AWS, elija Utilizar clave propiedad de AWS.
- Para utilizar su propia clave de AWS KMS, elija Elegir una AWS KMS key existente. Para cada región que haya seleccionado en el paso 3, elija una clave de AWS KMS o introduzca un `AWS KMSNombre de recurso de Amazon (ARN)`.

 Tip

Si no dispone de una AWS KMS key, elija Crear una AWS KMS key.

5. (Opcional) En el área Etiquetas, añada una o varias etiquetas al conjunto de réplica. Una etiqueta incluye una clave y, opcionalmente, un valor.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Para obtener más información, consulte [Etiquetado de recursos en Incident Manager](#).

6. (Opcional) En el área Acceso al servicio, para activar la característica Resultados, seleccione la casilla de verificación Crear rol de servicio de resultados en esta cuenta.

Un resultado es información sobre una implementación de código o un cambio en la infraestructura que se produjo alrededor del mismo momento en que se creó un incidente. Un resultado se puede examinar como una posible causa del incidente. La información sobre estas posibles causas se añade a la página Detalles del incidente del incidente. Con la información sobre estas implementaciones y cambios a mano, los respondedores no necesitan buscar manualmente esta información.

 Tip

Para ver información sobre el rol que se va a crear, elija Ver permisos.

7. Seleccione Crear.

Para obtener más información sobre conjuntos de réplica y capacidad de recuperación, consulte [Resiliencia en AWS Systems Manager Incident Manager](#).

Contactos (opcional)

1. Elija Crear contacto.

Incident Manager administra los contactos durante un incidente. Para obtener más información sobre los contactos, consulte [Uso de los contactos en Incident Manager](#).


2. En Nombre, introduzca el nombre del contacto.
3. En Alias único, introduzca un alias para identificar a este contacto.
4. En la sección Canal del contacto, haga lo siguiente para definir cómo se involucra al contacto durante los incidentes:
 - a. En Tipo, elija Correo electrónico, SMS o Voz.
 - b. En Nombre del canal, introduzca un nombre único que le ayude a identificar el canal.

- c. En Detalle, introduzca la dirección de correo electrónico o el número de teléfono del contacto.

Los números de teléfono deben tener entre 9 y 15 caracteres y empezar por + seguido del prefijo del país y el número de suscriptor.

- d. Para crear otro canal de contacto, seleccione Añadir un nuevo canal de contacto. Recomendamos definir al menos dos canales para cada contacto.

5. En el área Plan de participación, haga lo siguiente para definir a través de qué canales se notificará al contacto y cuánto tiempo se esperará para recibir un acuse de recibo a través de cada canal. Seleccione los canales de contacto que se utilizarán para interactuar con el contacto durante los incidentes.

 Note

Recomendamos definir al menos dos dispositivos en el plan de participación.

- a. En Nombre del canal de contacto, elija un canal que haya especificado en el área Canal de contacto.
- b. En Tiempo de participación (min), introduzca el número de minutos que se debe esperar antes de utilizar el canal de contacto.

Le recomendamos que seleccione al menos un dispositivo al que conectarse al principio de una participación, especificando 0 (cero) minutos de tiempo de espera.

- c. Para añadir más canales de contacto al plan de participación, elija Añadir participación.

6. (Opcional) En el área Etiquetas, añada una o varias etiquetas al contacto. Una etiqueta incluye una clave y, opcionalmente, un valor.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Para obtener más información, consulte [Etiquetado de recursos en Incident Manager](#).

7. Para crear el registro de contactos y enviar códigos de activación a los canales de contacto definidos, elija Siguiente.
8. (Opcional) En la página Activación del canal de contacto, introduzca el código de activación enviado a cada canal.

Puede generar nuevos códigos de activación más adelante si no puede introducirlos en este momento.

9. Repita el paso cuatro hasta que haya añadido todos sus contactos a Incident Manager.
10. Una vez introducidos todos los contactos, elija Finalizar.

(Opcional) Planes de escalada

1. Elija Crear plan de escalada.

Durante un incidente, un plan de escalada escala a través de sus contactos a fin de garantizar que Incident Manager implique a los respondedores correctos. Para obtener más información sobre los planes de escalada, consulte [Uso de los planes de escalada en Incident Manager](#).

2. En Nombre, introduzca un nombre único para el plan de escalada.
3. En Alias, introduzca un alias único que le ayude a identificar el plan de escalada.
4. En el área Etapa 1, haga lo siguiente:
 - a. En Canal de escalada, elija los canales de contacto que desee involucrar.
 - b. Si desea que un contacto pueda detener la progresión de las etapas del plan de escalada, seleccione El reconocimiento detiene la progresión del plan.
 - c. Para añadir más canales a una etapa, elija Añadir canal de escalada.
5. Para crear una nueva etapa en el plan de escalada, elija Añadir etapa y añada los detalles de su etapa.
6. (Opcional) En el área Etiquetas, añada una o varias etiquetas al plan de escalada. Una etiqueta incluye una clave y, opcionalmente, un valor.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Para obtener más información, consulte [Etiquetado de recursos en Incident Manager](#).

7. Elija Crear plan de escalada.

Plan de respuesta

1. Elija Crear plan de respuesta. Utilice el plan de respuesta para reunir los contactos y los planes de escalada que haya creado. Durante este asistente de Preparación, las siguientes secciones son opcionales, en especial si es la primera vez que configura un plan de respuesta:

- Canal de chat
- Manuales de procedimientos
- Participaciones
- Integraciones de terceros

Para obtener información sobre cómo añadir más adelante estos elementos a los planes de respuesta, consulte [Preparación para incidentes en Incident Manager](#).

2. En Nombre, introduzca un nombre único e identificable para el plan de respuesta. El nombre se utiliza para crear el ARN del plan de respuesta o en planes de respuesta sin nombre que mostrar.
3. (Opcional) En Nombre para mostrar, introduzca un nombre que le ayude a identificar este plan de respuesta al crear incidentes.
4. En Título, introduzca un título que le ayude a identificar el tipo de incidente que se relaciona con este plan de respuesta. El valor que especifique se incluye en el título de cada incidente. La alarma o evento que inició el incidente también se añade al título.
5. En Impacto, seleccione el nivel de impacto que espera de los incidentes relacionados con este plan de respuesta, como **Critical** o **Low**.
6. (Opcional) En Resumen, introduzca una breve descripción que ofrezca una visión general del incidente. Incident Manager rellena automáticamente la información relevante en el resumen durante un incidente.
7. (Opcional) En Cadena de deduplicación, introduzca una cadena de deduplicación. Incident Manager utiliza esta cadena para evitar que la misma causa raíz cree varios incidentes en la misma cuenta.

Una cadena de deduplicación es un término o frase que el sistema utiliza para buscar incidentes duplicados. Si especifica una cadena de deduplicación, Incident Manager busca incidentes abiertos que contengan la misma cadena en el campo `dedupeString` al crear el incidente. Si se detecta un duplicado, Incident Manager deduplica el incidente más reciente en el incidente existente.

Note

De forma predeterminada, Incident Manager deduplica automáticamente múltiples incidentes creados por la misma alarma de Amazon CloudWatch o evento de Amazon

EventBridge. No es necesario que introduzca su propia cadena de deduplicación para evitar la duplicación para estos tipos de recursos.

8. (Opcional) En el área Etiquetas, añada una o varias etiquetas al plan de respuesta. Una etiqueta incluye una clave y, opcionalmente, un valor.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Para obtener más información, consulte [Etiquetado de recursos en Incident Manager](#).

9. Seleccione los contactos y los planes de escalada que se aplicarán al incidente en el cuadro desplegable Participaciones.
10. Elija Crear plan de respuesta.

Una vez creado un plan de respuesta, puede asociar alarmas de Amazon CloudWatch o eventos de Amazon EventBridge al plan de respuesta. Esto creará automáticamente un incidente en función de una alarma o un evento. Para obtener más información, consulte [Creación de incidentes en Incident Manager](#).

Administración de incidentes entre regiones y entre cuentas en Incident Manager

Puede configurar Incident Manager, una capacidad de AWS Systems Manager, para que funcione con múltiples Regiones de AWS y cuentas. En esta sección se describen las prácticas recomendadas, los pasos de configuración y las limitaciones conocidas entre regiones y entre cuentas.

Temas

- [Administración de incidentes entre regiones](#)
- [Administración de incidentes entre cuentas](#)

Administración de incidentes entre regiones

Incident Manager admite la creación automatizada y manual de incidentes en [múltiples Regiones de AWS](#). Al incorporar por primera vez Incident Manager mediante el asistente Preparación, puede especificar hasta tres Regiones de AWS para su conjunto de réplica. Para incidentes creados automáticamente por alarmas de Amazon CloudWatch o eventos de Amazon EventBridge, Incident Manager intenta crear un incidente en la misma Región de AWS que la regla o alarma del evento. Si Incident Manager no está disponible en la Región de AWS, CloudWatch o EventBridge crearán automáticamente el incidente en una de las regiones disponibles especificadas en su conjunto de réplica.

Important

Tenga en cuenta los siguientes detalles importantes.

- Le recomendamos que especifique al menos dos Regiones de AWS en su conjunto de réplica. Si no especifica al menos dos regiones, el sistema no podrá crear incidentes durante el periodo en que Incident Manager no esté disponible.
- Los incidentes creados por una conmutación por error entre regiones no invocan los manuales de procedimientos especificados en los planes de respuesta.

Para obtener más información sobre la iniciación con Incident Manager y la especificación de regiones adicionales, consulte [Introducción a Incident Manager](#).

Administración de incidentes entre cuentas

Incident Manager utiliza AWS Resource Access Manager (AWS RAM) para compartir recursos de Incident Manager entre cuentas de administración y de aplicaciones. En esta sección se describen las prácticas recomendadas entre cuentas, cómo configurar la funcionalidad entre cuentas y las limitaciones conocidas de funcionalidad entre cuentas en Incident Manager.

Una cuenta de administración es la cuenta desde la que se administran las operaciones. En la configuración de una organización, la cuenta de administración es la propietaria de los planes de respuesta, los contactos, los planes de escalada, los manuales de procedimientos y otros recursos de AWS Systems Manager.

Una cuenta de aplicación es la cuenta propietaria de los recursos que componen sus aplicaciones. Estos recursos pueden ser instancias de Amazon EC2, tablas de Amazon DynamoDB o cualquiera de los otros recursos que utiliza para crear aplicaciones en la Nube de AWS. Las cuentas de aplicaciones también son propietarias de las alarmas de Amazon CloudWatch y los eventos de Amazon EventBridge que crean incidentes en Incident Manager.

AWS RAM utiliza el uso compartido de recursos para compartir recursos entre cuentas. Puede compartir el plan de respuesta y los recursos de contacto entre cuentas en AWS RAM. Al compartir estos recursos, las cuentas de aplicación y las cuentas de administración pueden interactuar con las participaciones y los incidentes. Al compartir un plan de respuesta se comparten todos los incidentes pasados y futuros creados mediante ese plan de respuesta. Al compartir un contacto se comparten todas las participaciones pasadas y futuras del contacto o del plan de respuesta.

Prácticas recomendadas

Observe estas prácticas recomendadas al compartir recursos de Incident Manager entre cuentas:

- Actualice regularmente el uso compartido de recursos con los planes de respuesta y los contactos.
- Revise regularmente las entidades principales del recurso compartido.
- Configure Incident Manager, los manuales de procedimientos y los canales de chat en su cuenta de administración.

Instalación y configuración de la administración de incidentes entre cuentas

Los siguientes pasos describen cómo instalar y configurar los recursos de Incident Manager y utilizarlos para la funcionalidad entre cuentas. Es posible que ya haya configurado anteriormente algunos servicios y recursos para la funcionalidad entre cuentas. Utilice estos pasos como una lista de comprobación de los requisitos antes de iniciar su primer incidente utilizando recursos entre cuentas.

1. (Opcional) Cree organizaciones y unidades organizativas con AWS Organizations. Siga los pasos del [Tutorial: Creación y configuración de una organización](#) en la Guía del usuario de AWS Organizations.
2. (Opcional) Utilice la función de configuración rápida de Systems Manager para configurar los roles de AWS Identity and Access Management correctos para que los utilice al configurar sus manuales de procedimientos entre cuentas. Para obtener más información, consulte [Configuración rápida](#) en la Guía del usuario de AWS Systems Manager.
3. Siga los pasos indicados en [Ejecución de automatizaciones en múltiples Regiones de AWS y cuentas](#) de la Guía del usuario de AWS Systems Manager para crear manuales de procedimientos en sus documentos de automatización de Systems Manager. Un manual de procedimientos puede ser ejecutado por una cuenta de administración o por una de sus cuentas de aplicación. En función de su caso de uso, necesitará instalar la plantilla de AWS CloudFormation adecuada para los roles necesarios a fin de crear y ver los manuales de procedimientos durante un incidente.
 - Ejecución de un manual de procedimientos en la cuenta de administración. La cuenta de administración debe descargar e instalar la plantilla de CloudFormation [AWS-SystemsManager-AutomationReadOnlyRole](#). Al instalar `AWS-SystemsManager-AutomationReadOnlyRole`, especifique los ID de cuenta de todas las cuentas de aplicaciones. Este rol permitirá a sus cuentas de aplicación leer el estado del manual de procedimientos desde la página de detalles del incidente. La cuenta de aplicación debe instalar la plantilla de CloudFormation [AWS-SystemsManager-AutomationAdministrationReadOnlyRole](#). La página de detalles del incidente utiliza este rol para obtener el estado de la automatización de la cuenta de administración.
 - Ejecución de un manual de procedimientos en una cuenta de aplicación. La cuenta de administración debe descargar e instalar la plantilla de CloudFormation [AWS-SystemsManager-AutomationAdministrationReadOnlyRole](#). Este rol permite a la cuenta de administración leer el estado del manual de procedimientos en la cuenta de aplicación. La cuenta de aplicación debe descargar e instalar la plantilla de

- CloudFormation [AWS-SystemsManager-AutomationReadOnlyRole](#). Al instalar `AWS-SystemsManager-AutomationReadOnlyRole`, especifique el ID de cuenta de la cuenta de administración y de otras cuentas de aplicación. La cuenta de administración y otras cuentas de aplicación asumen este rol para leer el estado del manual de procedimientos.
- (Opcional) En cada cuenta de aplicación de la organización, descargue e instale la plantilla de CloudFormation [AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole](#). Al instalar `AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole`, especifique el ID de cuenta de la cuenta de administración. Este rol proporciona los permisos que Incident Manager necesita para acceder a la información sobre las implementaciones de AWS CodeDeploy y las actualizaciones de la pila de AWS CloudFormation. Esta información se notifica como resultados de un incidente si la característica Resultados está habilitada. Para obtener más información, consulte [Uso de los resultados en Incident Manager](#).
 - Para configurar y crear contactos, planes de escalada, canales de chat y planes de respuesta, siga los pasos que se detallan en [Preparación para incidentes en Incident Manager](#).
 - Añada sus contactos y recursos de planes de respuesta a su recurso compartido existente o a un nuevo recurso compartido en AWS RAM. Para obtener más información, consulte el [Tutorial de introducción a AWS RAM](#) en la Guía del usuario de AWS RAM. La adición de planes de respuesta a AWS RAM permite a las cuentas de aplicación acceder a los incidentes y a los paneles de control de incidentes creados mediante los planes de respuesta. Las cuentas de aplicación también obtienen la capacidad de asociar alarmas de CloudWatch y eventos de EventBridge a un plan de respuesta. La adición de los contactos y los planes de escalado a AWS RAM permite a las cuentas de aplicación ver las participaciones e involucrar a los contactos desde el panel de control de incidentes.
 - Añada a su consola de CloudWatch la funcionalidad entre cuentas y entre regiones. Para conocer los pasos y obtener información, consulte [Consola de CloudWatch entre cuentas y entre regiones](#) en la Guía del usuario de Amazon CloudWatch. La adición de esta funcionalidad garantiza que las cuentas de la aplicación y la cuenta de administración que haya creado puedan ver y editar las métricas de los paneles de control de incidentes y análisis.
 - Cree un bus de eventos de Amazon EventBridge entre cuentas. Para conocer los pasos y obtener información, consulte [Envío y recepción de eventos de Amazon EventBridge entre cuentas de AWS](#). A continuación, puede utilizar este bus de eventos para crear reglas de eventos que detecten incidentes en las cuentas de aplicaciones y creen incidentes en la cuenta de administración.

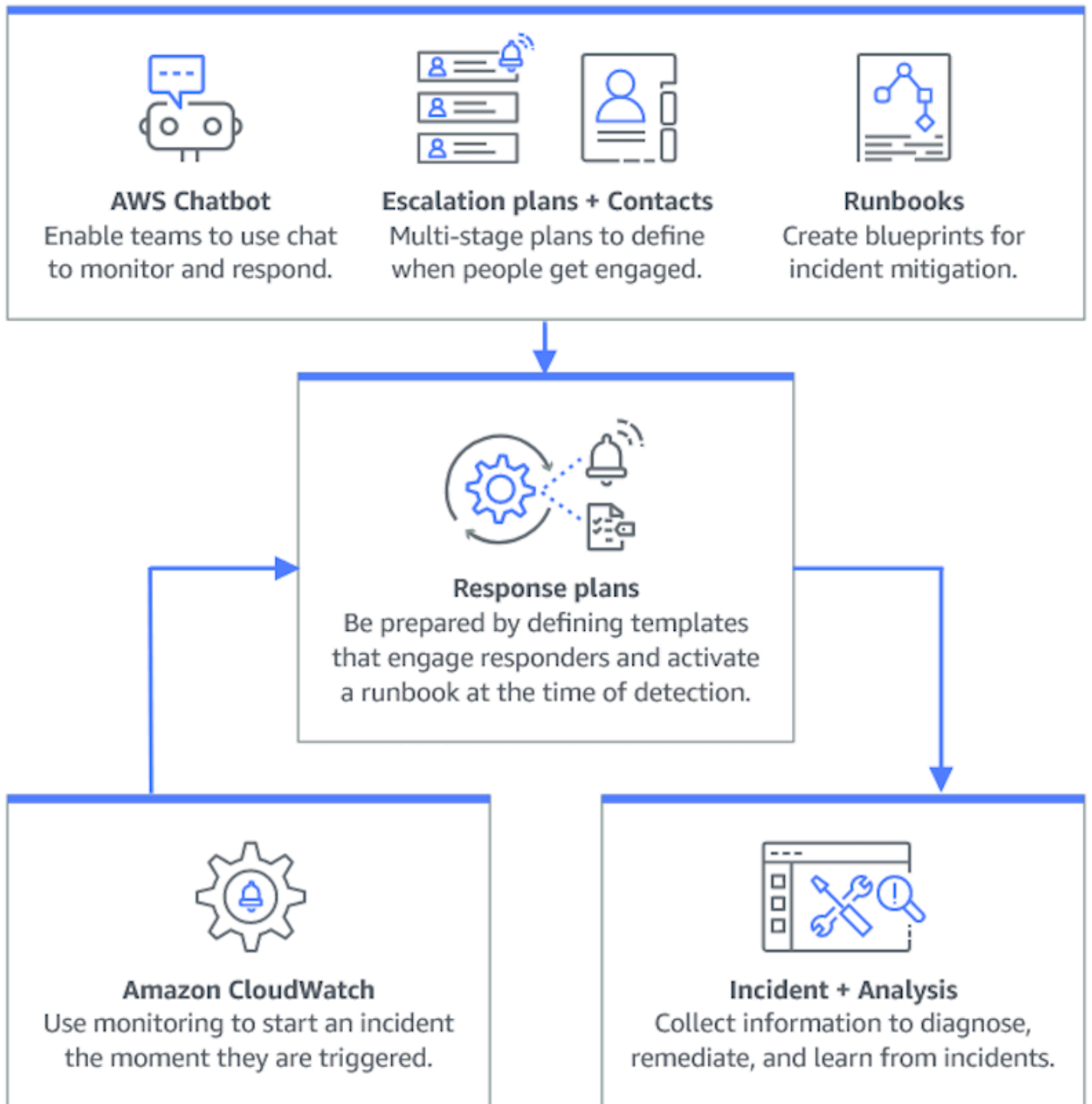
Limitaciones

A continuación se indican las limitaciones conocidas de la funcionalidad entre cuentas de Incident Manager:

- La cuenta que crea un análisis post-incidente es la única que puede verlo y modificarlo. Si utiliza una cuenta de aplicación para crear un análisis post-incidente, solo los miembros de esa cuenta podrán verlo y modificarlo. Lo mismo ocurre si utiliza una cuenta de administración para crear un análisis post-incidente.
- Los eventos de línea temporal no se rellenan para los documentos de automatización ejecutados en cuentas de aplicación. Las actualizaciones de los documentos de automatización ejecutados en las cuentas de aplicación son visibles en la pestaña Manual de procedimientos de la incidencia.
- Los temas de Amazon Simple Notification Service no se pueden utilizar entre cuentas. Los temas de Amazon SNS se deben crear en la misma región y cuenta que el plan de respuesta en el que se utiliza. Recomendamos utilizar la cuenta de administración para crear todos los temas de SNS y planes de respuesta.
- Los planes de escalada solo se pueden crear utilizando contactos de la misma cuenta. No es posible añadir un contacto que se haya compartido con usted a un plan de escalada de su cuenta.
- Las etiquetas aplicadas a los planes de respuesta, los registros de incidentes y los contactos solo pueden verse y modificarse desde la cuenta del propietario del recurso.

Preparación para incidentes en Incident Manager

La planificación de un incidente comienza mucho antes del ciclo de vida del incidente. A fin de prepararse para un incidente, tenga en cuenta cada uno de los siguientes temas antes de crear planes de respuesta. Utilice el monitoreo, los contactos, los planes de escalada, los canales de chat y los manuales de procedimientos para crear planes de respuesta que automaticen la respuesta.



Temas

- [Supervisión](#)
- [Uso de los ajustes generales](#)
- [Uso de los contactos en Incident Manager](#)

- [Uso de los horarios de guardia en Incident Manager](#)
- [Uso de los planes de escalada en Incident Manager](#)
- [Uso de los canales de chat en Incident Manager](#)
- [Uso de los manuales de procedimientos de Systems Manager Automation en Incident Manager](#)
- [Uso de los planes de respuesta en Incident Manager](#)
- [Uso de los resultados en Incident Manager](#)

Supervisión

Monitorear el estado de sus aplicaciones alojadas en AWS es clave para garantizar el tiempo operativo y el rendimiento de las aplicaciones. A la hora de determinar las soluciones de monitoreo, tenga en cuenta lo siguiente:

- Criticidad de la característica: si el sistema fallara, ¿cuán crítico sería el impacto para los usuarios intermedios?
- Comunalidad de los fallos: con qué frecuencia falla un sistema; los sistemas que requieren una intervención frecuente deben ser monitoreados de cerca.
- Aumento de la latencia: cuánto ha aumentado o disminuido el tiempo necesario para completar una tarea.
- Métricas del lado del cliente vs. métricas del lado del servidor: si existe una discrepancia entre las métricas relacionadas en el cliente y en el servidor.
- Fallos de dependencia: fallos para los que su equipo puede y debería prepararse.

Después de crear planes de respuesta, puede utilizar sus soluciones de monitoreo para hacer un seguimiento automático de los incidentes en el momento en que se produzcan en su entorno. Para obtener más información sobre el seguimiento y la creación de incidentes, consulte [Seguimiento de incidentes en Incident Manager](#).

Para obtener más información sobre cargas de trabajo y aplicaciones de infraestructura seguras, alto rendimiento, resistentes y eficientes, consulte el [documento técnico AWS Well-Architected](#).

Uso de los ajustes generales

Una vez que haya completado el asistente de incorporación de Incident Manager, puede administrar ciertas opciones en la página Configuración. Estas opciones incluyen su conjunto de réplica, las etiquetas aplicadas al conjunto de réplica y la característica Resultados.

Temas

- [Uso del conjunto de réplica de Incident Manager](#)
- [Administración de las etiquetas de un conjunto de réplica](#)
- [Administración de la característica Resultados](#)

Uso del conjunto de réplica de Incident Manager

El conjunto de réplica de Incident Manager replica sus datos en muchas Regiones de AWS para aumentar la redundancia entre regiones, permitir que Incident Manager acceda a recursos en diferentes regiones y reducir la latencia para sus usuarios. El conjunto de réplica también se utiliza para cifrar sus datos con una Clave administrada de AWS o con su propia clave administrada por el cliente. Todos los recursos de Incident Manager están cifrados de forma predeterminada. Para obtener más información sobre cómo se cifran sus recursos, consulte [Protección de los datos en Incident Manager](#). Para empezar a utilizar Incident Manager, cree primero su conjunto de réplica mediante el asistente Preparación. Para obtener más información sobre cómo prepararse en Incident Manager, consulte el [Asistente de preparación](#).

Edición de su conjunto de réplica

Puede editar su conjunto de réplica mediante la página Configuración de Incident Manager. Puede añadir o eliminar regiones y habilitar o deshabilitar la protección de borrado del conjunto de réplica. No puede editar la clave utilizada para cifrar sus datos. Para cambiar la clave, debe eliminar y volver a crear el conjunto de réplica.

Adición de una región

1. Abra la [consola de Incident Manager](#) y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. Elija Añadir región.
3. Seleccione la Región.
4. Elija Add (Agregar).

Eliminación de una región

1. Abra la [consola de Incident Manager](#) y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. Seleccione la región que desee eliminar.
3. Elija Eliminar.
4. Escriba delete (eliminar) en el cuadro de texto y elija Eliminar.

Eliminación de su conjunto de réplica

Al eliminar la última región en su conjunto de réplica se elimina el conjunto de réplica por completo. Antes de eliminar la última región, desactive Protección de borrado en la página Configuración para deshabilitar la protección de borrado. Después de eliminar su conjunto de réplica, puede crear un nuevo conjunto de réplica utilizando el asistente Preparación.

Para eliminar una región de su conjunto de réplica, debe esperar 24 horas después de crearla. Si intenta eliminar una región de su conjunto de réplica antes de que transcurran 24 horas desde su creación, la eliminación fallará.

Al eliminar su conjunto de réplica se eliminan todos los datos de Incident Manager.

Eliminación del conjunto de réplica

1. Abra la [consola de Incident Manager](#) y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. Seleccione la última región en su conjunto de réplica.
3. Elija Eliminar.
4. Escriba delete (eliminar) en el cuadro de texto y elija Eliminar.

Administración de las etiquetas de un conjunto de réplica

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Utilice etiquetas para categorizar un recurso de diferentes maneras, como por ejemplo, por finalidad, propietario o entorno.

Para administrar las etiquetas de un conjunto de réplica

1. Abra la [consola de Incident Manager](#) y, a continuación, elija Configuración en el panel de navegación izquierdo.

2. En el área Etiquetas, elija Editar.
3. Para añadir una etiqueta, haga lo siguiente:
 - a. Elija Add new tag (Agregar nueva etiqueta).
 - b. Escriba una clave y un valor opcional para la etiqueta.
 - c. Seleccione Guardar.
4. Para eliminar una etiqueta, haga lo siguiente:
 - a. Debajo de la etiqueta que desee eliminar, seleccione Eliminar.
 - b. Seleccione Guardar.

Administración de la característica Resultados

La característica Resultados ayuda a los respondedores de su organización a identificar las posibles causas raíz de los incidentes poco después de que estos comiencen. En la actualidad, Incident Manager proporciona resultados para implementaciones de AWS CodeDeploy y actualizaciones de pilas de AWS CloudFormation.

Para que los resultados sean compatibles en todas las cuentas, una vez habilitada la característica, deberá completar un paso de configuración adicional en cada cuenta de aplicación de la organización.

Para utilizar la característica, debe dejar que Incident Manager cree un rol de servicio que incluya los permisos necesarios para acceder a los datos en su nombre.

Para habilitar la característica Resultados

1. Abra la [consola de Incident Manager](#) y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. En el área Resultados, elija Crear rol de servicio.
3. Revise la información sobre el rol de servicio que va a crear y, a continuación, elija Crear.

Para deshabilitar la característica Resultados

Para dejar de utilizar la característica Resultados, elimine el rol `IncidentManagerIncidentAccessServiceRole` de cada cuenta en la que se haya creado.

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación izquierdo, seleccione Roles.
3. En el cuadro de búsqueda, escriba **IncidentManagerIncidentAccessServiceRole**.
4. Elija el nombre del rol y, a continuación, elija Eliminar.
5. Introduzca el nombre del rol en el cuadro de diálogo para confirmar que desea eliminarlo y, a continuación, elija Eliminar.

Uso de los contactos en Incident Manager

Los contactos de AWS Systems Manager Incident Manager son los respondedores ante incidentes. Un contacto puede tener varios canales que Incident Manager puede involucrar durante un incidente. Puede definir el plan de participación de un contacto a fin de describir cómo y cuándo Incident Manager se relaciona con el contacto.

Temas

- [Canales de contacto](#)
- [Planes de participación](#)
- [Creación de un contacto](#)
- [Importación de datos de contacto a su libreta de direcciones](#)

Canales de contacto

Los canales de contacto son los distintos métodos que utiliza Incident Manager para interactuar con un contacto.

Incident Manager admite los siguientes canales de contacto:

- Correo electrónico
- Servicio de mensajes cortos (SMS)
- Voz

Activación del canal de contacto

Para proteger su privacidad y seguridad, Incident Manager le envía un código de activación de dispositivos al crear contactos. Para utilizar sus dispositivos durante un incidente, primero debe

activarlos. Para ello, introduzca el código de activación del dispositivo en la página de creación de contactos.

Algunas características de Incident Manager incluyen funciones que envían notificaciones a un canal de contacto. Al utilizar estas características, usted da su consentimiento para que este servicio envíe notificaciones sobre interrupciones del servicio u otros eventos a los canales de contacto incluidos en el flujo de trabajo especificado. Esto incluye las notificaciones enviadas a un contacto como parte de una rotación de horario de guardia. Las notificaciones podrían enviarse por correo electrónico, mensaje SMS o llamada de voz, según se especifique en los datos de un contacto. Al utilizar estas características, usted confirma que está autorizado a añadir los canales de contacto que proporciona a Incident Manager.

Desactivación

Puede cancelar estas notificaciones en cualquier momento; para ello, elimine un dispositivo móvil como canal de contacto. Los destinatarios individuales de las notificaciones también pueden cancelar las notificaciones en cualquier momento eliminando el dispositivo de su contacto.

Para eliminar un canal de contacto de un contacto

1. Vaya a la [consola de Incident Manager](#) y elija Contactos en el panel de navegación izquierdo.
2. Seleccione el contacto con el canal de contacto que vaya a eliminar y elija Editar.
3. Elija Eliminar junto al canal de contacto que desea eliminar.
4. Elija Actualizar.

Desactivación del canal de contacto

Para desactivar un dispositivo, responda UNSUBSCRIBE. Al responder UNSUBSCRIBE, impide que Incident Manager controle su dispositivo.

Reactivación del canal de contacto

1. Responda START al mensaje de Incident Manager.
2. Vaya a la [consola de Incident Manager](#) y elija Contactos en el panel de navegación izquierdo.
3. Seleccione el contacto con el canal de contacto que vaya a eliminar y elija Editar.
4. Elija Activar dispositivos.
5. Introduzca el Código de activación enviado al dispositivo por Incident Manager.

6. Elija Activar.

Planes de participación

Los planes de participación definen cuándo Incident Manager utiliza los canales de contacto. Puede activar los canales de contacto varias veces en diferentes etapas desde el inicio de una intervención. Puede utilizar planes de participación en un plan de escalada o en un plan de respuesta. Para obtener más información sobre los planes de escalada, consulte [Uso de los planes de escalada en Incident Manager](#).

Creación de un contacto

Para crear un contacto, siga estos pasos.

1. Abra la [consola de Incident Manager](#) y elija Contactos en el panel de navegación izquierdo.
2. Elija Crear contacto.
3. Escriba el nombre completo del contacto y proporcione un alias único e identificable.
4. Defina un Canal de contacto. Le recomendamos que disponga de dos o más tipos diferentes de canales de contacto.
 - a. Elija el tipo: correo electrónico, SMS o voz.
 - b. Introduzca un nombre identificable para el canal de contacto.
 - c. Proporcione los detalles del canal de contacto, como el correo electrónico: arosalez@example.com.
5. Para definir más de un canal de contacto, elija Añadir canal de contacto. Repita el paso 4 para cada nuevo canal de contacto añadido.
6. Defina un plan de participación.

Important

Para involucrar a un contacto, debe definir un plan de participación.

- a. Elija un Nombre de canal de contacto.
- b. Defina cuántos minutos desde el inicio de la participación se debe esperar hasta que Incident Manager utilice este canal de contacto.

- c. Para añadir otro canal de contacto, elija Añadir participación.
7. Una vez definido el plan de participación, seleccione Crear. Incident Manager envía un código de activación a cada uno de los canales de contacto definidos.
8. (Opcional) Para activar los canales de contacto, introduzca el código de activación que Incident Manager envió a cada canal de contacto definido.
9. (Opcional) Para enviar un nuevo código de activación, seleccione Enviar nuevo código.
10. Elija Finalizar.

Después de definir un contacto y activar sus canales de contacto, puede añadir contactos a los planes de escalada para formar una cadena de escalado. Para obtener más información sobre los planes de escalada, consulte [Uso de los planes de escalada en Incident Manager](#). Puede añadir contactos a un plan de respuesta para lograr una participación directa. Para obtener más información sobre la creación de planes de respuesta, consulte [Uso de los planes de respuesta en Incident Manager](#).

Importación de datos de contacto a su libreta de direcciones

Al crearse un incidente, Incident Manager puede avisar a los respondedores mediante notificaciones de voz o SMS. Para garantizar que los respondedores vean que la llamada o la notificación por SMS procede de Incident Manager, recomendamos que todos los respondedores descarguen el archivo [formato de tarjeta virtual \(.vcf\)](#) de Incident Manager a la libreta de direcciones de sus dispositivos móviles. El archivo está alojado en Amazon CloudFront y disponible en la partición comercial de AWS.

Para descargar el archivo .vcf de Incident Manager

1. En su dispositivo móvil, elija o introduzca la siguiente URL: <https://d26vhuvd5b89k2.cloudfront.net/aws-incident-manager.vcf>.
2. Guarde o importe el archivo a la libreta de direcciones de su dispositivo móvil.

Uso de los horarios de guardia en Incident Manager

Un horario de guardia en Incident Manager define a quién se notifica al producirse un incidente que requiera la intervención de un operario. Un horario de guardia consta de una o más rotaciones que usted crea para el horario. Cada rotación puede incluir hasta 30 contactos.

Después de crear un horario de guardia, puede incluirlo como una escalada en su plan de escalada. Al producirse un incidente asociado a ese plan de escalada, Incident Manager lo notifica al operador (u operadores) de guardia según el horario. Este contacto puede entonces dar reconocimiento de su participación. En su plan de escalada, puede designar uno o más horarios de guardia, así como uno o más contactos individuales, a través de múltiples etapas de escalado. Para obtener más información, consulte [Uso de los planes de escalada en Incident Manager](#).

Tip

Como práctica recomendada, le sugerimos que añada contactos y horarios de guardia como canales de escalada en un plan de escalada. A continuación, debe elegir un plan de escalada como la participación en un plan de respuesta. Este enfoque proporciona la cobertura más completa para la respuesta a incidentes en su organización.

Cada horario de guardia admite hasta ocho rotaciones. Las rotaciones pueden superponerse o ejecutarse de forma concurrente. Esto aumenta el número de operadores notificados para responder al producirse un incidente. También puede crear rotaciones que se ejecuten consecutivamente. Esto admite escenarios como la administración de incidentes “follow-the-sun” (jornada continua) en la que tiene grupos en todo el mundo que dan soporte al mismo servicio.

Utilice los temas de esta sección como ayuda para crear y administrar horarios de guardia para sus operaciones de respuesta a incidentes.

Temas

- [Creación de un horario de guardia y rotaciones en Incident Manager](#)
- [Administración de un horario de guardia existente en Incident Manager](#)

Creación de un horario de guardia y rotaciones en Incident Manager

Cree un horario de guardia con una o varias rotaciones de contactos a los que contactar para responder a incidentes durante sus turnos.

Antes de empezar

Antes de crear un horario de guardia, asegúrese de haber creado previamente los contactos que desea añadir a las rotaciones del horario. Para obtener información, consulte [Uso de los contactos en Incident Manager](#).

Consideración de los cambios de horario de verano (DST)

Al crear una rotación, usted especifica la zona horaria global que sirve de base para las horas de cobertura de turnos y las fechas para esta rotación. Puede utilizar cualquier zona horaria definida por la [Autoridad de Números Asignados en Internet \(Internet Assigned Numbers Authority, IANA\)](#). Por ejemplo, America/Los_Angeles, UTC y Asia/Seoul. Puede añadir más de una rotación a un horario de guardia. Sin embargo, si los respondedores de cada rotación se encontrasen geográficamente en zonas horarias diferentes, tenga en cuenta cualquier cambio de horario de verano al que podría estar sujeta cada rotación.

Por ejemplo, America/Los_Angeles y Europe/Dublin observan horarios de verano diferentes. Como resultado, la diferencia horaria entre las dos zonas puede variar de 6 a 8 horas según la época del año. Por ejemplo, un horario de guardia “follow-the-sun” tiene una rotación en la zona horaria America/Los_Angeles y otra en Europe/Dublin. En este ejemplo, el horario puede contener una brecha de turnos de una hora o un solapamiento de turnos de una hora debido a los cambios por horario de verano.

Para evitar estas situaciones, le recomendamos el siguiente enfoque:

1. Utilice una única zona horaria para todas las rotaciones en un horario de guardia.
2. Calcule las horas locales al asignar respondedores fuera de esa zona horaria en particular.

Si decide asignar cada rotación a su zona horaria local, revise el horario antes que cualquier horario de verano. A continuación, ajuste los horarios de rotación de turnos según sea necesario para asegurarse de evitar brechas o solapamientos involuntarios en su cobertura de guardia antes de que entre en vigor cualquier cambio de horario de verano.

Para crear un horario de guardia

1. Abra la [consola de Incident Manager](#).
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. Elija Crear horario de guardia.
4. En Nombre del horario, introduzca un nombre que le ayude a identificar el horario, como **MyApp Primary On-call Schedule**.
5. En Alias del horario, introduzca un alias para este horario que sea único en la Región de AWS actual, como **my-app-primary-on-call-schedule**.

6. (Opcional) En el área Etiquetas, aplique uno o más pares de nombre clave y valor de etiqueta al horario de guardia.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Por ejemplo, puede etiquetar un horario para identificar el periodo en que se ejecuta, los tipos de operadores que contiene o el plan de escalada que admita. Para obtener más información sobre el etiquetado de recursos de Incident Manager, consulte [Etiquetado de recursos en Incident Manager](#).

7. Realice a continuación la [adición de una o más rotaciones al plan de guardia](#).

Creación de una rotación para un plan de guardia en Incident Manager

Una rotación en un programa de guardia especifica cuándo está vigente el turno. También especifica los contactos que rotan en los turnos. Puede incluir hasta ocho rotaciones en un único programa de guardia.

En una rotación puede añadir a cualquier persona que haya creado como contacto en Incident Manager. Para obtener información sobre la administración de sus contactos, consulte [Uso de los contactos en Incident Manager](#).

A medida que configura su rotación, puede ver el aspecto general del horario en un calendario de Vista previa en la parte derecha de la página.

Para crear una rotación en un horario de guardia

1. En la sección Rotación 1 de la página Crear horario de guardia, en Nombre de la rotación, introduzca un nombre que identifique la rotación, como **00:00 - 7:59 Support** o **Dublin Support Group**.
2. En Fecha de inicio, introduzca la fecha en la que se activa esta rotación en formato YYYY/MM/DD, como 2023/07/14.
3. En Zona horaria, seleccione la zona horaria global que sirve de base para las horas de cobertura de turnos y las fechas que especifique para esta rotación.

Puede utilizar cualquier zona horaria definida por la Autoridad de Números Asignados en Internet (Internet Assigned Numbers Authority, IANA). Por ejemplo: “America/Los_Angeles”, “UTC”, “Asia/Seoul”. Para obtener más información, consulte la [base de datos de zonas horarias](#) en el sitio web de IANA.

⚠ Warning

Puede basar cada rotación en su propia zona horaria. Sin embargo, cualquier cambio por horario de verano en las zonas horarias que seleccione puede afectar a sus ventanas de cobertura previstas. Para obtener más información, consulte [Consideración de los cambios de horario de verano \(DST\)](#), tratado anteriormente en este tema.

4. En Hora de inicio de la rotación, introduzca la hora a la que comienza el turno de esta rotación en formato hh:mm de 24 horas, como 16:00.

Tenga en cuenta las diferencias en la hora local para los contactos que se encuentren en zonas horarias distintas a la que ha especificado. Por ejemplo, si elige America/Los_Angeles como zona horaria y 00:00 como hora de inicio de la rotación, esto equivale a las 08:00 en Dublín (Irlanda) y a las 13:30 en Bombay (India).

5. En Hora de finalización de la rotación, introduzca la hora a la que finaliza el turno de esta rotación en formato hh:mm de 24 horas, como 23:59.

ℹ Note

El tiempo entre el inicio y el final de una rotación debe ser de al menos 30 minutos.

6. (Opcional) Para establecer la duración de la rotación en 24 horas, elija Cobertura de 24 horas e introduzca la hora de inicio de esta rotación en el campo Hora de inicio de la rotación. El valor de Hora de finalización de la rotación se actualiza automáticamente.

Por ejemplo, si desea que su guardia tenga una cobertura de 24 horas con el cambio de turno a las 11:00 (11 AM), seleccione Cobertura de 24 horas e introduzca **11:00** como hora de inicio.

7. En Días activos, seleccione los días de la semana en los que esta rotación estará activa. Por ejemplo, si su plan de guardia excluye la cobertura de fin de semana, seleccione todos los días excepto sábado y domingo.
8. Realice a continuación la [Adición de contactos a la rotación](#).

Adición de contactos a una rotación en un horario de guardia en Incident Manager

Para cada rotación de su programa de guardia, puede añadir uno o varios contactos, hasta un total de 30. Puede elegir entre los contactos establecidos en la configuración de Incident Manager.

Al añadir un contacto a una rotación, este puede recibir notificaciones como parte de sus obligaciones de guardia. Las notificaciones pueden enviarse por correo electrónico, SMS o llamada de voz, según se especifique en los datos del contacto.

Para obtener información sobre cómo administrar los contactos y las opciones de notificación de contactos, consulte [Uso de los contactos en Incident Manager](#).

Para añadir contactos a una rotación en un programa de guardia

1. En la página Crear horario de guardia, en la sección Contactos de la rotación, elija Añadir o eliminar contactos.
2. En el cuadro de diálogo Añadir o eliminar contactos, seleccione los alias de los contactos que desee incluir en la rotación.

El orden en que seleccione los contactos es el orden en que aparecen por primera vez en el calendario de rotación. Puede cambiar el orden de los contactos después de añadirlos.

3. Elija Confirmar.
4. Para cambiar la posición de orden de un contacto, seleccione el botón de opción correspondiente a ese usuario y utilice los botones Arriba y Abajo para actualizar el orden de los contactos.
5. Realice a continuación la [Especificación de periodicidad y duración de los turnos individuales](#) para la rotación.

Especificación de periodicidad y duración de los turnos y adición de etiquetas a una rotación en Incident Manager

La periodicidad de los turnos especifica la frecuencia con la que los contactos de una rotación entran y salen de la guardia. Una duración de periodicidad se puede especificar en número de días, semanas o meses.

Para especificar la periodicidad y duración de los turnos y añadir etiquetas a una rotación

1. En la página Crear horario de guardia, en la sección Configuración de periodicidad de la rotación, haga lo siguiente:

- En Tipo de periodicidad del turno, especifique si cada turno de guardia dura un número de días, semanas o meses eligiendo entre Daily, Weekly y Monthly.
- En Duración del turno, introduzca cuántos días, semanas o meses dura un turno.

Por ejemplo, si elige Daily e introduce **1**, el turno de guardia de cada contacto dura un día. Si elige Weekly e introduce **3**, el turno de guardia de cada contacto dura tres semanas.

2. (Opcional) En el área Etiquetas, aplique uno o más pares de nombre clave y valor de etiqueta a la rotación.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Por ejemplo, puede etiquetar una rotación para identificar la ubicación de los contactos asignados a ella, el tipo de cobertura que debe proporcionar o el plan de escalada que respaldará. Para obtener más información sobre el etiquetado de recursos de Incident Manager, consulte [Etiquetado de recursos en Incident Manager](#).

3. (Recomendado) Utilice la vista previa del calendario para asegurarse de que no haya brechas involuntarias en la cobertura de su plan de guardia.
4. Seleccione Crear.

Ahora puede añadir el horario de guardia como canal de escalada en un plan de escalada. Para obtener información, consulte [Creación de un plan de escalada](#).

Administración de un horario de guardia existente en Incident Manager

Utilice el contenido de esta sección como ayuda para trabajar con los horarios de guardia que ya haya creado.

Temas

- [Visualización de detalles del horario de guardia](#)
- [Edición de un horario de guardia](#)
- [Copia de un horario de guardia](#)
- [Creación de una anulación para una rotación del horario de guardia](#)
- [Eliminación de un horario de guardia](#)

Visualización de detalles del horario de guardia

Puede acceder a un resumen general de un horario de guardia en la página Ver detalles del horario de guardia. Esta página también contiene información sobre quién está actualmente de guardia y quién lo estará a continuación. La página incluye una vista de calendario que muestra qué contactos están de guardia en un momento determinado.

Para ver los detalles de un horario de guardia

1. Abra la [consola de Incident Manager](#).
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. En la fila del horario de guardia que desee ver, realice una de las siguientes acciones:

- Para abrir una vista resumida del calendario, elija el alias del horario.

-o bien-

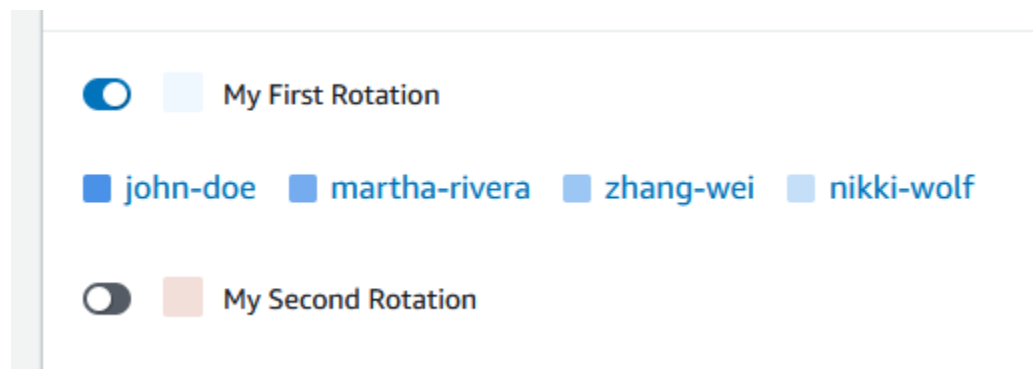
Seleccione el botón de opción de la fila y luego elija Ver.

- Para abrir una vista de calendario del horario, elija Ver calendario



En la vista de calendario, elija el nombre de un contacto en una fecha específica del horario para ver los detalles sobre el turno asignado o crear una anulación.

- Para activar o desactivar la visualización de una rotación específica en el calendario, accione el interruptor situado junto al nombre de la rotación.



Edición de un horario de guardia

Puede actualizar la configuración de un horario de guardia y sus rotaciones, excepto los siguientes detalles:

- El alias del horario
- Los nombres de las rotaciones
- Las fechas de inicio de las rotaciones


Para utilizar un calendario existente como base para un nuevo calendario con la posibilidad de cambiar estos valores, puede copiar el calendario en cuestión. Para obtener información, consulte [Copia de un horario de guardia](#).

Para editar un horario de guardia

1. Abra la [consola de Incident Manager](#).
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. Haga una de las siguientes acciones:
 - Seleccione el botón de opción en la fila del horario de guardia que desee editar y luego elija Editar.
 - Seleccione el alias del horario de guardia para abrir la página Ver detalles del horario de guardia y luego elija Editar.
4. Realice las modificaciones necesarias en el horario de guardia y sus rotaciones. Puede cambiar las opciones de configuración de las rotaciones, como las horas de inicio y fin, los contactos y la periodicidad. Puede añadir o eliminar rotaciones del horario según sea necesario. La vista previa del calendario refleja sus cambios a medida que los realiza.

Para obtener información sobre cómo utilizar las opciones de la página, consulte [Creación de un horario de guardia y rotaciones en Incident Manager](#).

5. Elija Actualizar.

 Important

Si edita un horario que contiene anulaciones, sus cambios pueden afectar a las anulaciones. Para asegurarse de que sus anulaciones permanezcan configuradas de la forma esperada, le recomendamos que revise detenidamente sus anulaciones de turnos después de actualizar el horario.

Copia de un horario de guardia

Para utilizar la configuración de un horario de guardia existente como punto de partida para un nuevo horario, puede crear una copia del horario y modificarla según sea necesario.

Para copiar un horario de guardia

1. Abra la [consola de Incident Manager](#).
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. Seleccione el botón de opción en la fila del horario de guardia que desee copiar.
4. Elija Copiar.
5. Realice las modificaciones necesarias en el calendario y sus rotaciones. Puede cambiar, añadir o eliminar rotaciones según sea necesario.

Note

Al copiar un horario existente, debe especificar nuevas fechas de inicio para cada rotación. Los horarios copiados no admiten rotaciones con fechas de inicio en el pasado.

Para obtener información sobre cómo utilizar las opciones de la página, consulte [Creación de un horario de guardia y rotaciones en Incident Manager](#).

6. Elija Crear copia.

Creación de una anulación para una rotación del horario de guardia

Si necesita realizar cambios puntuales en un programa de rotación existente, puede crear una anulación. Una anulación le permite sustituir el turno de un contacto, de forma total o parcial, por otro contacto. También puede crear una anulación que abarque varios turnos.

Solo puede asignar a una anulación contactos que ya estén asignados a la rotación.

En la vista previa del calendario, los turnos anulados se muestran con un fondo con franja en vez de un fondo sólido. En la siguiente imagen, se puede ver que el contacto Zhang Wei está de guardia en una anulación que incluye partes de los turnos de John Doe y Martha Rivera, con inicio el 5 de mayo y fin el 11 de mayo.

On-call schedule details Info

Edit Delete

Schedule details
Schedule calendar


May 2023
↻ Create override ◀ Today ▶

America/Los_Angeles (local timezone)


Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	May 01	02	03	04	05	06
	00:00 - 23:59 zhang-wei	00:00 - 23:59 zhang-wei	00:00 - 23:59 john-doe	00:00 - 23:59 john-doe	00:00 - 23:59 zhang-wei	
07	08	09	10	11	12	13
	00:00 - 23:59 zhang-wei	00:00 - 23:59 zhang-wei	00:00 - 23:59 zhang-wei	00:00 - 23:59 zhang-wei	00:00 - 23:59 martha-rivera	
14	15	16	17	18	19	20
	00:00 - 23:59 martha-rivera	00:00 - 23:59 martha-rivera	00:00 - 23:59 zhang-wei	00:00 - 23:59 zhang-wei	00:00 - 23:59 zhang-wei	

Para crear una anulación de un horario de guardia

1. Abra la [consola de Incident Manager](#).
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. En la fila del horario de guardia que desee ver, realice una de las siguientes acciones:
 - Elija el alias del horario y, a continuación, la pestaña Calendario del horario.
 - Elija Ver calendario


4. Haga una de las siguientes acciones:
 - Elija Crear anulación.

- Elija el nombre de un contacto en la vista previa del calendario y, a continuación, elija Anular turno.
5. En el cuadro de diálogo Crear anulación de turno, haga lo siguiente:

 Note

Una anulación debe tener una duración mínima de 30 minutos. Solo puede especificar una anulación para turnos que tengan lugar como máximo seis meses en el futuro.

- a. En Seleccionar rotación, seleccione el nombre de la rotación en la que desea crear una anulación.
 - b. En Fecha de inicio, seleccione o introduzca la fecha en la que comienza la anulación.
 - c. En Hora de inicio, introduzca la hora de inicio de la anulación en formato hh:mm.
 - d. En Fecha de finalización, seleccione o introduzca la fecha en la que finaliza la anulación.
 - e. En Hora de finalización, introduzca la hora a la que finaliza la anulación, en formato hh:mm.
 - f. En Seleccionar contacto de anulación, seleccione el nombre del contacto de rotación que estará de guardia durante el periodo de anulación.
6. Elija Crear anulación.

Después de crear una anulación, puede identificarla por su fondo con franja. Al elegir el nombre del contacto de un turno anulado, un cuadro de información lo identifica como turno anulado. Puede elegir Eliminar anulación para eliminarla y restaurar la asignación de guardia original.

Eliminación de un horario de guardia

Cuando ya no necesite un determinado horario de guardia, puede eliminarlo de Incident Manager.

Si algún plan de escalada o de respuesta utiliza actualmente el horario de guardia como canal de escalada, deberá eliminarlo de esos planes para poder eliminar el horario.

Para eliminar un horario de guardia

1. Abra la [consola de Incident Manager](#).
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. Seleccione el botón de opción en la fila del horario de guardia que desee eliminar.

4. Elija Eliminar.
5. En el cuadro de diálogo ¿Eliminar horario de guardia?, introduzca **confirm** en el cuadro de texto.
6. Elija Eliminar.

Uso de los planes de escalada en Incident Manager

AWS Systems Manager Incident Manager proporciona rutas de escalada a través de sus contactos u horarios de guardia definidos, conocidos colectivamente como canales de escalada. Puede incorporar múltiples canales de escalada a un incidente al mismo tiempo. Si los contactos designados en el canal de escalada no responden, Incident Manager escala al siguiente conjunto de contactos. También puede elegir si un plan deja de escalar una vez que un usuario reconoce la participación. Puede añadir planes de escalada a un plan de respuesta para que la escalada comience automáticamente al principio de un incidente. También puede añadir planes de escalada a un incidente activo.

Temas

- [Escenarios](#)
- [Creación de un plan de escalada](#)

Escenarios

Los planes de escalada utilizan etapas en las que cada una dura un número definido de minutos. Cada etapa tiene la siguiente información:

- **Duración:** la cantidad de tiempo que el plan espera hasta comenzar la siguiente etapa. La primera etapa del plan de escalada comienza una vez iniciada la participación.
- **Canal de escalada:** un canal de escalada es un contacto único o un horario de guardia compuesto por varios contactos que rotan responsabilidades según un horario definido. El plan de escalada compromete a cada canal utilizando su plan de participación definido. Puede configurar cada canal de escalada para detener la progresión del plan de escalada antes de que continúe a la siguiente etapa. Cada etapa puede tener múltiples canales de escalada.

Para obtener información sobre la configuración de contactos individuales, consulte [Uso de los contactos en Incident Manager](#). Para obtener información sobre la creación de horarios de guardia, consulte [Uso de los horarios de guardia en Incident Manager](#).

Creación de un plan de escalada

1. Abra la [consola de Incident Manager](#) y elija Planes de escalada en el panel de navegación izquierdo.
2. Elija Crear plan de escalada.
3. En Nombre, introduzca un nombre único para el plan de escalada, como **My Escalation Plan**.
4. En Alias, introduzca un alias que le ayude a identificar el plan, como **my-escalation-plan**.
5. En Duración de la etapa, introduzca el número de minutos que debe esperar Incident Manager hasta pasar a la siguiente etapa.
6. En Canal de escalada, elija uno o varios contactos u horarios de guardia para que participen durante esta etapa.
7. (Opcional) Para permitir que un contacto detenga el plan de escalada una vez que reconozca la participación, seleccione El reconocimiento detiene la progresión del plan.
8. Para añadir otro canal a esta etapa, elija Añadir canal de escalada.
9. Para añadir otra etapa al plan de escalada, elija Añadir etapa.
10. Repita los pasos 5 a 9 hasta que termine de añadir los canales de escalada y las etapas que desee para este plan de escalada.
11. (Opcional) En el área Etiquetas, aplique uno o más pares de nombre clave y valor de etiqueta al plan de escalada.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Por ejemplo, puede etiquetar un plan de escalada para identificar el tipo de incidente para el cual se utilizará, los tipos de canales de escalada que contiene o el plan de escalada que admite. Para obtener más información sobre el etiquetado de recursos de Incident Manager, consulte [Etiquetado de recursos en Incident Manager](#).

12. Elija Crear plan de escalada.

Uso de los canales de chat en Incident Manager

Incident Manager, una capacidad de AWS Systems Manager, ofrece a los respondedores de incidentes la posibilidad de comunicar directamente a través de canales de chat durante un incidente.

Un canal de chat es una sala de chat que usted configura en [AWS Chatbot](#). A continuación, conecta este canal a un plan de respuesta en Incident Manager.

Durante un incidente, los respondedores utilizan el canal de chat para comunicar entre sí sobre el incidente. Incident Manager también envía las actualizaciones y notificaciones sobre el incidente directamente al canal de chat. Envía estas notificaciones utilizando uno o varios temas de Amazon Simple Notification Service (Amazon SNS) que especifique en la configuración del canal de chat.

AWS Chatbot e Incident Manager son compatibles con los canales de chat de las siguientes aplicaciones:

- Slack
- Microsoft Teams
- Amazon Chime

El proceso de configuración de un canal de chat para utilizarlo en sus incidentes consta de tareas en tres servicios diferentes de Amazon Web Services.

Tareas

- [Tarea 1: Crear o actualizar temas de Amazon SNS para su canal de chat](#)
- [Tarea 2: Crear un canal de chat en AWS Chatbot](#)
- [Tarea 3: Añadir el canal de chat a un plan de respuesta en Incident Manager](#)
- [Interacción a través del canal de chat](#)

Tarea 1: Crear o actualizar temas de Amazon SNS para su canal de chat

Amazon SNS es un servicio administrado que brinda la entrega de mensajes de los publicadores a los suscriptores (también conocidos como productores y consumidores). Los publicadores se comunican de forma asíncrona con los suscriptores mediante el envío mensajes a un tema, que es un punto de acceso lógico y un canal de comunicación. Incident Manager utiliza uno o varios temas que usted asocia a un plan de respuesta para enviar notificaciones sobre un incidente a los respondedores del mismo.

En un plan de respuesta, puede incluir uno o varios temas de Amazon SNS en las notificaciones de incidentes. Como práctica recomendada, debe crear un tema de SNS en cada Región de AWS que haya añadido a su conjunto de réplica.

i Tip

Para un flujo de trabajo de configuración más directo, le recomendamos que configure primero sus temas de Amazon SNS para utilizarlos con Incident Manager. Una vez configurados, puede crear el canal de chat.

Para crear o actualizar temas de Amazon SNS para su canal de chat

1. Siga los pasos indicados en [Creación de un tema de Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

i Note

Después de crear el tema, edítelo para actualizar su política de acceso.

2. Seleccione el tema que ha creado y anote o copie el nombre de recurso de Amazon (ARN) del tema, en un formato como `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
3. Elija Editar y, a continuación, expanda la sección Política de acceso para configurar permisos de acceso adicionales más allá de los predeterminados.
4. Añada la siguiente declaración a la matriz Declaración de la política:

```
{
  "Sid": "IncidentManagerSNSPublishingPermissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "ssm-incidents.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "sns-topic-arn",
  "Condition": {
    "StringEqualsIfExists": {
      "AWS:SourceAccount": "account-id"
    }
  }
}
```

Sustituya los *valores del marcador de posición* de la siguiente manera:

- *sns-topic-arn* es el nombre de recurso de Amazon (ARN) del tema que creó para esta región, en formato `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
 - *account-id* es el ID de la Cuenta de AWS en que trabaja, como 111122223333.
5. Elija Guardar cambios.
 6. Repita el proceso en cada región incluida en su conjunto de réplica.

Tarea 2: Crear un canal de chat en AWS Chatbot

Puede crear un canal de chat en Slack, Microsoft Teams o Amazon Chime. Solo necesita un canal de chat para cada plan de respuesta.

Para sus canales de chat, le recomendamos seguir el principio de privilegio mínimo (no proporcionar a los usuarios más permisos de los necesarios para completar sus tareas). También debería revisar periódicamente la membresía de sus canales de chat de AWS Chatbot. Las revisiones ayudan a comprobar que solo los respondedores apropiados y otras partes interesadas tengan acceso a sus canales de chat.

En los canales de Microsoft Teams y de Slack habilitados para AWS Chatbot, los respondedores de incidentes pueden ejecutar una serie de comandos de la CLI de Incident Manager directamente desde la aplicación Microsoft Teams o Slack. Para obtener más información, consulte [Interacción a través del canal de chat](#).

Important

Los usuarios que añada a su canal de chat deben ser los mismos contactos que figuran en su plan de escalada o de respuesta. También puede añadir usuarios adicionales a los canales de chat, como partes interesadas y observadores de incidentes.

Para obtener información general sobre AWS Chatbot, consulte [Qué es AWS Chatbot](#) en la Guía del administrador de AWS Chatbot.

Elija entre las siguientes aplicaciones en las que crear su canal:

Slack

Los pasos indicados en este procedimiento proporcionan la configuración de permisos recomendada para permitir que todos los usuarios del canal utilicen los comandos de chat con

Incident Manager. Al utilizar comandos de chat compatibles, sus respondedores de incidentes pueden actualizar e interactuar con el incidente directamente desde el canal de chat de Slack. Para obtener información, consulte [Interacción a través del canal de chat](#).

Para crear un canal de chat en Slack

- Siga los pasos indicados en [Tutorial: Introducción a Slack](#) en la Guía del administrador de AWS Chatbot e incluya lo siguiente en su configuración.
 - En el paso 10, en Configuración de roles, elija Rol del canal.
 - En el paso 10d, en Plantillas de políticas, seleccione Permisos de Incident Manager.
 - En el paso 11, en Políticas de barreras de protección del canal, en Nombre de la política, elija [AWSIncidentManagerResolverAccess](#).
 - En el paso 12, en la sección Temas de SNS, haga lo siguiente:
 - En Región 1, seleccione una Región de AWS que esté incluida en su conjunto de réplica.
 - En Temas 1, seleccione el tema de SNS que creó en esa región para utilizarlo para enviar notificaciones de incidentes al canal de chat.
 - Para cada región adicional en su conjunto de réplica, seleccione Añadir otra región y añada las regiones y los temas de SNS adicionales.

Microsoft Teams

Los pasos indicados en este procedimiento proporcionan la configuración de permisos recomendada para permitir que todos los usuarios del canal utilicen los comandos de chat con Incident Manager. Al utilizar comandos de chat compatibles, sus respondedores de incidentes pueden actualizar e interactuar con el incidente directamente desde el canal de chat de Microsoft Teams. Para obtener información, consulte [Interacción a través del canal de chat](#).

Para crear un canal de chat en Microsoft Teams

- Siga los pasos indicados en [Tutorial: Introducción a Microsoft Teams](#) en la Guía del administrador de AWS Chatbot e incluya lo siguiente en su configuración.
 - En el paso 10, en Configuración de roles, elija Rol del canal.
 - En el paso 10d, en Plantillas de políticas, seleccione Permisos de Incident Manager.

- En el paso 11, en Políticas de barreras de protección del canal, en Nombre de la política, elija [AWSIncidentManagerResolverAccess](#).
- En el paso 12, en la sección Temas de SNS, haga lo siguiente:
 - En Región 1, seleccione una Región de AWS que esté incluida en su conjunto de réplica.
 - En Temas 1, seleccione el tema de SNS que creó en esa región para utilizarlo para enviar notificaciones de incidentes al canal de chat.
 - Para cada región adicional en su conjunto de réplica, seleccione Añadir otra región y añada las regiones y los temas de SNS adicionales.

Amazon Chime

Para crear un canal de chat en Amazon Chime

- Siga los pasos indicados en [Tutorial: Introducción a Amazon Chime](#) en la Guía del administrador de AWS Chatbot e incluya lo siguiente en su configuración.
 - En el paso 11, en Plantillas de políticas, seleccione Permisos de Incident Manager.
 - En el paso 12, en la sección Temas de SNS, seleccione los temas de SNS que enviarán notificaciones al webhook de Amazon Chime:
 - En Región 1, seleccione una Región de AWS que esté incluida en su conjunto de réplica.
 - En Temas 1, seleccione el tema de SNS que creó en esa región para utilizarlo para enviar notificaciones de incidentes al canal de chat.
 - Para cada región adicional en su conjunto de réplica, seleccione Añadir otra región y añada las regiones y los temas de SNS adicionales.

Note

Los comandos de chat, que los respondedores de incidentes pueden utilizar en los canales de chat de Slack y Microsoft Teams, no son compatibles con Amazon Chime.

Tarea 3: Añadir el canal de chat a un plan de respuesta en Incident Manager

Al crear o actualizar un plan de respuesta, puede añadir canales de chat para que los respondedores comuniquen y reciban actualizaciones a través de ellos.

Al seguir los pasos de [Creación de un plan de respuesta](#), en la sección [\(Opcional\) Especificación de un canal de chat de respuesta a incidentes](#), seleccione el canal que desee utilizar para los incidentes relacionados con este plan de respuesta.

Interacción a través del canal de chat

Para los canales en Slack y Microsoft Teams, Incident Manager habilita a los respondedores a interactuar con los incidentes directamente desde el canal de chat utilizando los siguientes comandos `ssm-incidents`:

- [start-incident](#)
- [list-response-plan](#)
- [get-response-plan](#)
- [create-timeline-event](#)
- [delete-timeline-event](#)
- [get-incident-record](#)
- [get-timeline-event](#)
- [list-incident-records](#)
- [list-timeline-events](#)
- [list-related-items](#)
- [update-related-items](#)
- [update-incident-record](#)
- [update-timeline-event](#)

Para ejecutar comandos en el canal de chat de un incidente activo, utilice el siguiente formato. Sustituya *cli-options* por cualquier opción que desee incluir para un comando.

```
@aws ssm-incidents cli-options
```


Por ejemplo:

```
@aws ssm-incidents start-incident --response-plan-arn arn:aws:ssm-incidents::111122223333:response-plan/test-response-plan-chat --region us-east-2
```

```
@aws ssm-incidents create-timeline-event --event-data "\"example timeline event\"" --event-time 2023-03-31 T20:30:00.000 --event-type Custom Event --incident-record-arn arn:aws:ssm-incidents::111122223333:incident-record/MyResponsePlanChat/98c397e6-7c10-aa10-9b86-f199aEXAMPLE
```

```
@aws ssm-incidents list-incident-records
```

Uso de los manuales de procedimientos de Systems Manager Automation en Incident Manager

Puede utilizar manuales de procedimientos de [automatización de AWS Systems Manager](#), una capacidad de AWS Systems Manager, para automatizar tareas comunes de aplicaciones e infraestructuras en su entorno de Nube de AWS.

Cada manual de procedimientos define un flujo de trabajo del manual de procedimientos, que se compone de acciones que Systems Manager realiza en sus nodos administrados o en otros tipos de recursos de AWS. Puede utilizar los manuales de procedimientos para automatizar el mantenimiento, la implementación y la corrección de sus recursos de AWS.

En Incident Manager, un manual de procedimientos dirige la respuesta y mitigación de incidentes, y usted especifica un manual de procedimientos para utilizarlo como parte de un plan de respuesta.

En sus planes de respuesta, puede elegir entre docenas de manuales de procedimientos preconfigurados para tareas automatizadas habituales, o puede crear manuales de procedimientos personalizados. Al especificar un manual de procedimientos en la definición de un plan de respuesta, el sistema puede iniciarlo automáticamente al producirse un incidente.

Important

Los incidentes creados por una conmutación por error entre regiones no invocan los manuales de procedimientos especificados en los planes de respuesta.

Para obtener más información sobre Systems Manager Automation, los manuales de procedimientos y el uso de los mismos con Incident Manager, consulte los siguientes temas:

- Para añadir un manual de procedimientos a un plan de respuesta, consulte [Uso de los planes de respuesta en Incident Manager](#).
- Para obtener más información sobre los manuales de procedimientos, consulte [Automatización de AWS Systems Manager](#) en la Guía del usuario de AWS Systems Manager y la [Referencia del manual de procedimientos de automatización de AWS Systems Manager](#).
- Para obtener información sobre el costo de uso de los manuales de procedimientos, consulte [Precios de Systems Manager](#).
- Para obtener información sobre la invocación automática de manuales de procedimientos al crearse un incidente mediante una alarma de Amazon CloudWatch o un evento de Amazon EventBridge, consulte [Tutorial: Uso de manuales de procedimientos de Systems Manager Automation con Incident Manager](#).

Temas

- [Permisos de IAM necesarios para iniciar y ejecutar flujos de trabajo de manuales de procedimientos](#)
- [Uso de los parámetros del manual de procedimientos](#)
- [Definición de un manual de procedimientos](#)
- [Plantilla de manual de procedimientos de Incident Manager](#)

Permisos de IAM necesarios para iniciar y ejecutar flujos de trabajo de manuales de procedimientos

Incident Manager requiere permisos para ejecutar manuales de procedimientos como parte de su respuesta a incidentes. Para proporcionar estos permisos, utiliza los roles de AWS Identity and Access Management (IAM), el Rol de servicio Runbook, y la Automatización de *AssumeRole*.

El rol de servicio Runbook es un rol de servicio obligatorio. Este rol proporciona a Incident Manager los permisos que necesita para acceder e iniciar el flujo de trabajo del manual de procedimientos.

El *AssumeRole* de automatización proporciona los permisos necesarios para ejecutar los comandos individuales especificados dentro del manual de procedimientos.

Note

Si no se especifica ningún `AssumeRole`, Systems Manager Automation intenta utilizar el rol de servicio Runbook para los comandos individuales. Si no especifica un `AssumeRole`, debe añadir los permisos necesarios al rol de servicio Runbook. Si no lo hace, el manual de procedimientos no podrá ejecutar esos comandos.

Sin embargo, como práctica recomendada en materia de seguridad, recomendamos utilizar un `AssumeRole` separado. Con un `AssumeRole` separado, puede limitar los permisos necesarios que debe añadir a cada rol.

Para obtener más información sobre el `AssumeRole` de automatización, consulte [Configuración de un rol de servicio \(asumir rol\) de acceso para automatizaciones](#) en la Guía del usuario de AWS Systems Manager.

Puede crear usted mismo de forma manual cualquiera de los dos tipos de rol en la consola de IAM. También puede dejar que Incident Manager cree cualquiera de los dos por usted al crear o actualizar un plan de respuesta.

Permisos del rol de servicio Runbook

Los permisos del rol de servicio Runbook se proporcionan a través de una política similar a la siguiente.

La primera declaración permite a Incident Manager iniciar la operación `StartAutomationExecution` de Systems Manager. A continuación, esta operación se ejecuta en los recursos representados por los tres formatos de nombre de recurso de Amazon (ARN).

La segunda declaración permite que el rol de servicio Runbook asuma un rol en otra cuenta cuando ese manual de procedimientos se ejecuta en la cuenta afectada. Para obtener más información, consulte [Ejecución de automatizaciones en múltiples Regiones de AWS y cuentas](#) en la Guía del usuario de AWS Systems Manager.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartAutomationExecution",
```

```

    "Resource": [
      "arn:aws:ssm:*:{{DocumentAccountId}}:automation-definition/{{DocumentName}}:*",
      "arn:aws:ssm:*:{{DocumentAccountId}}:document/{{DocumentName}}:*",
      "arn:aws:ssm:*:automation-definition/{{DocumentName}}:*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-AutomationExecutionRole",
    "Condition": {
      "StringEquals": {
        "aws:CalledViaLast": "ssm.amazonaws.com"
      }
    }
  }
}

```

Permisos AssumeRole de automatización

Al crear o actualizar un plan de respuesta, puede elegir entre varias políticas administradas de AWS para vincular al AssumeRole que crea Incident Manager. Estas políticas proporcionan permisos para ejecutar una serie de operaciones comunes utilizadas en los escenarios del manual de procedimientos de Incident Manager. Puede elegir una o más de estas políticas administradas para proporcionar permisos a su política AssumeRole. En la siguiente tabla se describen las políticas entre las que puede elegir al crear un AssumeRole desde la consola de Incident Manager.

Nombre de la política administrada de AWS	Descripción de la política
AmazonSSMAutomationRole	Concede permisos para que el servicio de Systems Manager Automation ejecute las actividades definidas en los manuales de procedimientos. Asigne esta política a los administradores y a los usuarios de confianza avanzados.
AWSIncidentManagerResolverAccess	Concede permiso a los usuarios para iniciar, ver y actualizar incidentes. También puede utilizarlas para crear eventos de línea temporal

Nombre de la política administrada de AWS	Descripción de la política
	de clientes y elementos relacionados en el panel de control de incidentes.

Puede utilizar estas políticas administradas para conceder permisos para muchos escenarios comunes de respuesta a incidentes. Sin embargo, los permisos requeridos para las tareas específicas que necesite pueden variar. En estos casos, debe proporcionar permisos de políticas adicionales para su `AssumeRole`. Para obtener información, consulte la [Referencia del manual de procedimientos de automatización de AWS Systems Manager](#).

Uso de los parámetros del manual de procedimientos

Cuando se añade un manual de procedimiento a un plan de respuesta, se pueden especificar los parámetros que el manual debe utilizar en tiempo de puesta en marcha. Los planes de respuesta admiten parámetros con valores tanto estáticos como dinámicos. Para los valores estáticos, se introduce el valor cuando se define el parámetro en el plan de respuesta. En el caso de los valores dinámicos, el sistema determina el valor correcto del parámetro recopilando información del incidente. Incident Manager es compatible con los siguientes parámetros dinámicos:

Incident ARN

Cuando Incident Manager crea un incidente, el sistema captura el nombre de recurso de Amazon (ARN) del registro de incidentes correspondiente y lo ingresa para este parámetro en el manual de procedimiento.

Note

Este valor solo puede asignarse a parámetros de tipo `String`. Si se asigna a un parámetro de cualquier otro tipo, el manual no se pone en marcha.

Involved resources

Cuando Incident Manager crea un incidente, el sistema captura los ARN de los recursos involucrados en el incidente. Estos recursos ARN se asignan a este parámetro en el manual de procedimiento.

Acerca de los recursos asociados

Incident Manager puede rellenar los valores de los parámetros del manual de procedimientos con los ARN de los recursos de AWS especificados en alarmas de CloudWatch, eventos de EventBridge e incidentes creados manualmente. En esta sección se describen los distintos tipos de recursos para los que Incident Manager puede capturar ARN al rellenar este parámetro.

Alarmas de CloudWatch

Al crearse un incidente a partir de una acción de alarma de CloudWatch, Incident Manager extrae automáticamente los siguientes tipos de recursos de las métricas asociadas. A continuación, rellena los parámetros elegidos con los siguientes recursos implicados:

Servicio de AWS	Tipo de recurso
Amazon DynamoDB	Índices secundarios globales flujos Tablas
Amazon EC2	Imágenes Instancias
AWS Lambda	Aliases de rol Versiones de funciones Funciones
Amazon Relational Database Service (Amazon RDS)	Clústeres Instancias de base de datos
Amazon Simple Storage Service (Amazon S3)	Buckets

Reglas de EventBridge

Cuando el sistema crea un incidente a partir de un evento de EventBridge, Incident Manager rellena los parámetros elegidos con la propiedad `Resources` del evento. Para obtener más información, consulte [Eventos de Amazon EventBridge](#) en la Guía del usuario de Amazon EventBridge.

Incidentes creados manualmente

Al crear un incidente mediante la acción [StartIncident](#) de la API, Incident Manager rellena los parámetros elegidos utilizando la información de la llamada a la API. En concreto, rellena los parámetros utilizando elementos de tipo `INVOLVED_RESOURCE` que se pasan en el parámetro `relatedItems`.

Note

El valor `INVOLVED_RESOURCES` solo puede asignarse a parámetros de tipo `StringList`. Si se asigna a un parámetro de cualquier otro tipo, el manual no se pone en marcha.

Definición de un manual de procedimientos

Al crear un manual de procedimientos, puede seguir los pasos que se proporcionan aquí, o seguir la guía más detallada que se proporciona en la sección [Uso de los manuales de procedimientos](#) de la Guía del usuario de Systems Manager. Si va a crear un manual de procedimientos para varias cuentas y regiones, consulte [Ejecución de automatizaciones en múltiples Regiones de AWS y cuentas](#) en la Guía del usuario de Systems Manager.

Definición de un manual de procedimientos

1. Abra la consola de Administrador de sistemas en <https://console.aws.amazon.com/systems-manager/>.
2. En el panel de navegación, elija Documentos.
3. Elija Create automation (Crear automatización).
4. Introduzca un nombre de manual de procedimientos único e identificable.
5. Introduzca una descripción del manual de procedimientos.
6. Proporcione un rol de IAM para que el documento de automatización lo asuma. Esto permite al manual de procedimientos ejecutar comandos automáticamente. Para obtener más información, consulte [Configuración de un acceso de rol de servicio para flujos de trabajo de automatización](#).
7. (Opcional) Añada cualquier parámetro de entrada con el que se inicie el manual de procedimientos. Puede utilizar parámetros dinámicos o estáticos al iniciar un manual de

- procedimientos. Los parámetros dinámicos utilizan valores del incidente en el que se inicia el manual de procedimientos. Los parámetros estáticos utilizan el valor que usted proporciona.
8. (Opcional) Añada un tipo de Objetivo.
 9. (Opcional) Añada etiquetas.
 10. Complete los pasos que el manual de procedimientos seguirá al ejecutarse. Cada paso requiere:
 - Un nombre.
 - Una descripción del propósito del paso.
 - La acción que se va a ejecutar durante el paso. Los manuales de procedimientos utilizan el tipo de acción Pausa para describir un paso manual.
 - (Opcional) Propiedades del comando.
 11. Después de añadir todos los pasos necesarios del manual de procedimientos, elija Crear automatización.

Para habilitar la funcionalidad multicuentas, comparta el manual de procedimientos de su cuenta de administración con todas las cuentas de la aplicación que utilicen el manual de procedimientos durante un incidente.

Uso compartido de un manual de procedimientos

1. Abra la consola de Administrador de sistemas en <https://console.aws.amazon.com/systems-manager/>.
2. En el panel de navegación, elija Documents.
3. En la lista de documentos, elija el documento que desee compartir y, a continuación, elija Ver detalles. En la pestaña Permissions (Permisos), verifique que es usted el propietario del documento. Solo el propietario del documento puede compartirlo.
4. Elija Editar.
5. Para compartir el comando públicamente, seleccione Public (Público) y, a continuación, Save (Guardar). Para compartir el comando de forma privada, elija Private (Privado), ingrese el ID de Cuenta de AWS, elija Add permission (Agregar permiso) y, a continuación, elija Save (Guardar).

Plantilla de manual de procedimientos de Incident Manager

Incident Manager proporciona la siguiente plantilla de manual de procedimientos para ayudar a su equipo a empezar a crear manuales de procedimientos en Systems Manager Automation.

Puede utilizar esta plantilla tal cual o editarla para incluir detalles específicos de su aplicación y sus recursos.

Localización de la plantilla de manual de procedimientos de Incident Manager

1. Abra la consola de Administrador de sistemas en <https://console.aws.amazon.com/systems-manager/>.
2. En el panel de navegación, elija Documents.
3. En el área Documentos, introduzca **AWSIncidents-** en el campo de búsqueda para mostrar todos los manuales de procedimientos de Incident Manager.

Tip

Introduzca **AWSIncidents-** como texto libre en lugar de utilizar la opción de filtro Prefijo de nombre de documento.

Uso de una plantilla

1. Abra la consola de Administrador de sistemas en <https://console.aws.amazon.com/systems-manager/>.
2. En el panel de navegación, elija Documentos.
3. Elija la plantilla que desee actualizar en la lista de documentos.
4. Elija la pestaña Contenido y, a continuación, copie el contenido del documento.
5. En el panel de navegación, elija Documentos.
6. Elija Create automation (Crear automatización).
7. Introduzca un nombre único e identificable.
8. Elija la pestaña Editor.
9. Elija Editar.
10. Pegue o introduzca los datos copiados en el área Editor de documentos.
11. Elija Create automation (Crear automatización).

AWSIncidents-CriticalIncidentRunbookTemplate

AWSIncidents-CriticalIncidentRunbookTemplate es una plantilla que proporciona el ciclo de vida de Incident Manager en pasos manuales. Estos pasos son suficientemente genéricos como para utilizarlos en la mayoría de las aplicaciones, pero también suficientemente detallados como para que los respondedores puedan iniciarse en la resolución de incidentes.

Uso de los planes de respuesta en Incident Manager

Los planes de respuesta le permiten planificar cómo responder a un incidente que afecte a sus usuarios. Un plan de respuesta funciona como una plantilla que incluye información sobre a quién involucrar, la gravedad prevista del suceso, los manuales de procedimientos automáticos por iniciar y las métricas por monitorear.

Prácticas recomendadas

Puede reducir el impacto de los incidentes en sus equipos al planificarlos con antelación. Los equipos deberían tener en cuenta las siguientes prácticas recomendadas al diseñar un plan de respuesta.

- **Participación racionalizada:** identifique el equipo más apropiado para un incidente. Si involucra una lista de distribución demasiado amplia, o si involucra a equipos equivocados, podría causar confusión y hacer perder tiempo a los respondedores durante un incidente.
- **Escalada fiable:** para sus compromisos en un plan de respuesta, le recomendamos que seleccione un plan de participación en vez de contactos u horarios de guardia. El plan de participación debe especificar los contactos individuales o los horarios de guardia (que contienen múltiples contactos rotativos) que debe involucrar durante los incidentes. Dado que los respondedores especificados en su plan de participación podrían resultar inaccesibles en ocasiones, deberá configurar respondedores de reserva en su plan de respuesta para cubrir estos escenarios. Con contactos de reserva, si los contactos principal y secundario no estuvieran disponibles o hubiera otras lagunas no planificadas en la cobertura, Incident Manager seguirá notificando el incidente a un contacto.
- **Manuales de procedimientos:** utilice los manuales de procedimientos para proporcionar pasos repetibles y comprensibles que reduzcan el estrés que experimenta un respondedor durante un incidente.
- **Colaboración:** utilice los canales de chat para agilizar la comunicación durante los incidentes. Los canales de chat ayudan a los respondedores a mantenerse al día con la información. También pueden compartir información con otros respondedores a través de estos canales.

Creación de un plan de respuesta

Utilice el siguiente procedimiento para crear un plan de respuesta y automatizar la respuesta a incidentes.

Para crear un plan de respuesta

1. Abra la [consola de Incident Manager](#) y, en el panel de navegación, elija Planes de respuesta.
2. Elija Crear plan de respuesta.
3. En Nombre, introduzca un nombre del plan de respuesta único e identificable para utilizarlo en el nombre de recurso de Amazon (ARN) para el plan de respuesta.
4. (Opcional) En Nombre para mostrar, introduzca un nombre más legible para las personas que le ayude a identificar el plan de respuesta al crear incidentes.
5. Realice a continuación la [Especificación de valores predeterminados para los registros de incidentes](#).

Especificación de valores predeterminados para incidentes


Para ayudarle a administrar los incidentes de forma más eficaz, puede especificar valores predeterminados. Incident Manager aplica estos valores a todos los incidentes que estén asociados a un plan de respuesta.

Para especificar valores predeterminados de incidentes

1. En Título, introduzca un título para este incidente que le ayude a identificarlo en la página de inicio de Incident Manager.
2. En Impacto, elija un nivel de impacto para indicar el alcance potencial de un incidente creado a partir de este plan de respuesta, como Crítico o Bajo. Para obtener información sobre los niveles de impacto en Incident Manager, consulte [Triage](#).
3. (Opcional) En Resumen, introduzca un breve resumen del tipo de incidente creado a partir de este plan de respuesta.
4. (Opcional) En Cadena de deduplicación, introduzca una cadena de deduplicación. Incident Manager utiliza esta cadena para evitar que la misma causa raíz cree varios incidentes en la misma cuenta.

Una cadena de deduplicación es un término o frase que el sistema utiliza para buscar incidentes duplicados. Si especifica una cadena de deduplicación, Incident Manager busca incidentes

abiertos que contengan la misma cadena en el campo `dedupeString` al crear el incidente. Si se detecta un duplicado, Incident Manager deduplica el incidente más reciente en el incidente existente.

 Note

De forma predeterminada, Incident Manager deduplica automáticamente múltiples incidentes creados por la misma alarma de Amazon CloudWatch o evento de Amazon EventBridge. No es necesario que introduzca su propia cadena de deduplicación para evitar la duplicación para estos tipos de recursos.

5. (Opcional) En Etiquetas de incidentes, añada claves y valores de etiqueta para asignar a los incidentes creados por este plan de respuesta.


Debe tener el permiso `TagResource` para el recurso de registro de incidentes a fin de establecer etiquetas de incidentes dentro del plan de respuesta.

6. Realice a continuación la [Especificación de un canal de chat opcional](#) para que los respondedores comuniquen entre sí acerca de los incidentes.

(Opcional) Especificación de un canal de chat de respuesta a incidentes

Al incluir un canal de chat en un plan de respuesta, los respondedores reciben las actualizaciones del incidente a través del canal. Pueden interactuar con el incidente directamente desde el canal de chat utilizando comandos de chat.

Con AWS Chatbot, puede crear un canal para Slack o Amazon Chime a fin de utilizarlo en sus planes de respuesta. Para obtener información sobre la creación de un canal de chat en AWS Chatbot, consulte la [Guía del administrador de AWS Chatbot](#).

 Important

Incident Manager debe tener permisos para publicar en el tema de Amazon Simple Notification Service (Amazon SNS) de un canal de chat. Sin permisos para publicar en ese tema de SNS, no podrá añadirlo al plan de respuesta. Incident Manager publica una notificación de prueba en el tema de SNS para verificar los permisos.

Para obtener más información sobre los canales de chat, consulte [Uso de los canales de chat en Incident Manager](#).

Para especificar un canal de chat de respuesta a incidentes

1. En Canal de chat, elija un canal de chat de AWS Chatbot en el que los respondedores puedan comunicar durante un incidente.

 Tip

Para crear un nuevo canal de chat en AWS Chatbot, elija Configurar nuevo cliente Chatbot.

2. En Temas de SNS del canal de chat, elija temas de SNS adicionales en los que publicar durante el incidente. Añadir temas de SNS en varias Regiones de AWS aumenta la redundancia en caso de que una región esté caída en el momento del incidente.
3. Realice a continuación la [Selección de contactos, horarios de guardia y planes de escalada](#) que se activarán durante un incidente.

(Opcional) Selección de recursos que se activarán en una respuesta a incidentes

Es importante identificar a los respondedores más apropiados al producirse un incidente. Como práctica recomendada, le sugerimos que haga lo siguiente:

1. Añada contactos y horarios de guardia como los canales de escalada en un plan de escalada.
2. Elija un plan de escalada como compromiso en un plan de respuesta.

Para obtener más información sobre contactos y planes de escalada, consulte [Uso de los contactos en Incident Manager](#) y [Uso de los planes de escalada en Incident Manager](#).

Para seleccionar los recursos por involucrar en la respuesta a incidentes

1. En Participaciones, elija cualquier número de planes de escalada, programas de guardia y contactos individuales.
2. Como opción, realice a continuación la [Especificación de un manual de procedimientos para ejecutar](#) como parte de su mitigación de incidentes.

(Opcional) Especificación de un manual de procedimientos para mitigación de incidentes

Puede utilizar manuales de procedimientos de [automatización de AWS Systems Manager](#), una capacidad de AWS Systems Manager, para automatizar tareas comunes de aplicaciones e infraestructuras en su entorno de Nube de AWS.

Cada manual de procedimientos define un flujo de trabajo del manual de procedimientos. Un flujo de trabajo del manual de procedimientos incluye las acciones que Systems Manager realiza en sus nodos administrados o en otros tipos de recursos de AWS. En Incident Manager, un manual de procedimientos administra la respuesta y mitigación de incidentes.

Para obtener más información sobre el uso de manuales de procedimientos en los planes de respuesta, consulte [Uso de los manuales de procedimientos de Systems Manager Automation en Incident Manager](#).

Para especificar un manual de procedimientos para mitigación de incidentes:

1. En Manual de procedimientos, realice una de las siguientes acciones:
 - Elija Clonar manual de procedimientos de una plantilla para hacer una copia del manual de procedimientos predeterminado de Incident Manager. En Nombre, introduzca un nombre descriptivo para el nuevo manual de procedimientos.
 - Elija Seleccionar manual de procedimientos existente. Seleccione el Propietario, el Manual de procedimientos y la Versión que desee utilizar.

Tip

Para crear un manual de procedimientos desde cero, elija Configurar nuevo manual de procedimientos.


Para obtener más información acerca de la creación de manuales de procedimientos, consulte [Uso de los manuales de procedimientos de Systems Manager Automation en Incident Manager](#).

2. En el área Parámetros, introduzca los parámetros solicitados para el manual de procedimientos que haya seleccionado.

Los parámetros disponibles son los especificados por el manual de procedimientos. Un manual de procedimientos podría requerir parámetros distintos a los de otro manual. Algunos parámetros podrían ser obligatorios y otros opcionales.

En muchos casos, puede optar por introducir manualmente un valor estático para un parámetro, como una lista de ID de instancia de Amazon EC2. También puede permitir que Incident Manager proporcione los valores de los parámetros generados dinámicamente por un incidente.

3. (Opcional) En `AutomationAssumeRole`, especifique el rol de AWS Identity and Access Management (IAM) que se vaya a utilizar. Este rol debe tener los permisos necesarios para ejecutar los comandos individuales especificados dentro del manual de procedimientos.


 Note

Si no se especifica `AssumeRole`, Incident Manager intentará utilizar el rol de servicio Runbook para ejecutar los comandos individuales especificados dentro del manual de procedimientos.

Elija una de las siguientes opciones:

- Introducir valor de ARN: introduzca manualmente el nombre de recurso de Amazon (ARN) de un `AssumeRole`, en el formato `arn:aws:iam::account-id:role/assume-role-name`. Por ejemplo, `arn:aws:iam::123456789012:role/MyAssumeRole`.
- Utilizar un rol de servicio existente: elija un rol con los permisos requeridos de una lista de roles existentes en su cuenta.
- Crear nuevo rol de servicio: elija entre políticas administradas de AWS para vincular a su `AssumeRole`. Tras seleccionar esta opción, en Políticas administradas de AWS, elija una o más políticas en la lista.

Puede aceptar el nombre predeterminado sugerido para el nuevo rol o introducir uno que usted elija.

 Note

Este nuevo rol de servicio Runbook está asociado con el manual de procedimientos específico que haya seleccionado. No se puede utilizar con manuales de

procedimientos diferentes. Esto se debe a que la sección de recursos de la política no admite otros manuales de procedimientos.

4. En Rol de servicio Runbook, especifique el rol de IAM que se utilizará para proporcionar los permisos necesarios para acceder e iniciar el flujo de trabajo del manual de procedimientos en sí.

Como mínimo, el rol debe permitir la acción `ssm:StartAutomationExecution` para su manual de procedimientos específico. Para que el manual de procedimientos funcione en todas las cuentas, el rol también debe permitir la acción `sts:AssumeRole` para el rol `AWS-SystemsManager-AutomationExecutionRole` que creó durante [Administración de incidentes entre regiones y entre cuentas en Incident Manager](#).

Elija una de las siguientes opciones:

- Crear nuevo rol de servicio: Incident Manager crea un rol de servicio Runbook para usted que incluye los permisos mínimos necesarios para iniciar el flujo de trabajo del manual de procedimientos.

En Nombre del rol, puede aceptar el nombre predeterminado sugerido o introducir uno que usted elija. Le recomendamos que utilice el nombre sugerido o que mantenga el nombre del manual de procedimientos en el nombre. Esto se debe a que el nuevo AssumeRole está asociado con el manual de procedimientos específico que ha seleccionado y puede que no incluya los permisos necesarios para otros manuales de procedimientos.

- Utilizar rol de servicio existente: un rol de IAM creado previamente por usted o por Incident Manager otorga los permisos necesarios.

En Nombre del rol, seleccione el nombre del rol existente que desee utilizar.

5. Expanda Opciones adicionales y seleccione una de las siguientes para especificar la Cuenta de AWS en que debe ejecutarse el flujo de trabajo del manual de procedimientos.
 - Cuenta del propietario del plan de respuesta: inicia el flujo de trabajo del manual de procedimientos en la Cuenta de AWS que lo creó.
 - Cuenta afectada: inicie el flujo de trabajo del manual de procedimientos en la cuenta que inició o notificó el incidente.

Elija Cuenta afectada cuando utilice Incident Manager para escenarios entre cuentas y el manual de procedimientos necesite acceder a los recursos de la cuenta afectada para corregirlos.

6. Como opción, realice a continuación la [Integración de un servicio de PagerDuty en el plan de respuesta](#).

(Opcional) Integración de un servicio de PagerDuty en el plan de respuesta

Para integrar un servicio de PagerDuty en el plan de respuesta

Al integrar Incident Manager con PagerDuty, PagerDuty crea un incidente correspondiente toda vez que Incident Manager cree un incidente. El incidente en PagerDuty utiliza el flujo de trabajo de paginación y las políticas de escalada que haya definido allí, además de las de Incident Manager. PagerDuty vincula los eventos de línea temporal de Incident Manager como notas en su incidente.

1. Expanda Integraciones de terceros y marque la casilla Habilitar integración de PagerDuty.
2. En Seleccionar secreto, seleccione el secreto en AWS Secrets Manager donde almacena las credenciales para acceder a su cuenta de PagerDuty.

Para obtener información sobre cómo almacenar sus credenciales de PagerDuty en un secreto del Administrador de secretos, consulte [Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager](#).

3. En Servicio de PagerDuty, seleccione el servicio de su cuenta de PagerDuty donde desea crear el incidente de PagerDuty.
4. Realice a continuación la [Adición de etiquetas opcionales y creación del plan de respuesta](#).

Adición de etiquetas y creación del plan de respuesta

Para añadir etiquetas y crear el plan de respuesta

1. (Opcional) En el área Etiquetas, aplique uno o más pares de nombre-valor de claves de etiqueta al plan de respuesta.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Con las etiquetas, puede categorizar un recurso de diferentes maneras, como por propósito, propietario o entorno.

Por ejemplo, es posible que desee etiquetar un plan de respuesta para identificar el tipo de incidente que debe mitigar, los tipos de canales de escalada que contiene o el plan de escalada que se le asociará. Para obtener más información sobre el etiquetado de recursos de Incident Manager, consulte [Etiquetado de recursos en Incident Manager](#).

2. Elija Crear plan de respuesta.

Uso de los resultados en Incident Manager

En Incident Manager, un resultado es información sobre una implementación de AWS CodeDeploy o una actualización de pila de AWS CloudFormation que se produjo alrededor del momento de un incidente y que implicó a uno o más recursos probablemente relacionados con el incidente. Cada resultado se puede examinar como una posible causa del incidente. La información sobre estas posibles causas se añade a la página Detalles del incidente de un incidente. Con la información sobre estas implementaciones y cambios a mano, los respondedores no necesitan buscar manualmente esta información. Esto reduce el tiempo necesario para evaluar las posibles causas, lo cual puede reducir el tiempo medio de recuperación (MTTR) de un incidente.

Actualmente, Incident Manager admite la recopilación de resultados de dos Servicios de AWS: [AWS CodeDeploy](#) y [AWS CloudFormation](#).

Los resultados son una característica opcional. Puede habilitarla en el [Asistente de preparación](#), al incorporarse por primera vez a Incident Manager, o más tarde en la [página Configuración](#).

Al habilitar la característica de resultados, Incident Manager crea un rol de servicio para usted. Este rol de servicio incluye los permisos necesarios para recuperar resultados de CodeDeploy y CloudFormation.

Para trabajar con resultados en un escenario entre cuentas, habilite la característica en la cuenta de administración. A continuación, cada cuenta de aplicación en una organización AWS Resource Access Manager (AWS RAM) debe crear un rol de servicio correspondiente.

Consulte los siguientes temas como ayuda para utilizar la característica Resultados.

Temas

- [Habilitación y creación de un rol de servicio de resultados](#)
- [Configuración de permisos para el soporte de resultados entre cuentas](#)

Habilitación y creación de un rol de servicio de resultados

Al habilitar la característica Resultados, Incident Manager crea un rol de servicio denominado `IncidentManagerIncidentAccessServiceRole` en su nombre. Este rol de servicio proporciona los permisos que Incident Manager necesita para recopilar información sobre las implementaciones de CodeDeploy y las actualizaciones de la pila de CloudFormation que se produjeron alrededor del momento en que se creó un incidente.

Note

Si utiliza Incident Manager con una organización, el rol de servicio se crea en la cuenta de administración. Para trabajar con resultados en otras cuentas de la organización, se debe crear el rol de servicio en cada cuenta de aplicación. Para obtener información sobre el uso de una plantilla de CloudFormation para crear este rol en sus cuentas de aplicación, consulte el paso 4 en [Instalación y configuración de la administración de incidentes entre cuentas](#).

Este rol de servicio está asociado a una política administrada de AWS. Para obtener información sobre los permisos de esta política, consulte [AWS política gestionada: AWSIncidentManagerIncidentAccessServiceRolePolicy](#).

Para obtener información sobre cómo habilitar los resultados durante el proceso de incorporación a Incident Manager, consulte [Introducción a Incident Manager](#).

Para obtener información sobre cómo habilitar los resultados una vez completado el proceso de incorporación, consulte [Administración de la característica Resultados](#).

Configuración de permisos para el soporte de resultados entre cuentas

Para utilizar la característica Resultados entre cuentas con una organización establecida en AWS RAM, cada cuenta de aplicación debe configurar los permisos para que Incident Manager asuma el rol de servicio de la cuenta de administración en su nombre.

Estos permisos se pueden configurar en una cuenta de aplicación mediante la implementación de una plantilla de AWS CloudFormation proporcionada por AWS, que crea el rol `IncidentManagerIncidentAccessServiceRole`.

Para obtener información sobre la descarga e implementación de esta plantilla en una cuenta de aplicación, consulte el paso 4 de [Administración de incidentes entre regiones y entre cuentas en Incident Manager](#).

Creación de incidentes en Incident Manager

Incident Manager, una capacidad de AWS Systems Manager, le ayuda a administrar y responder rápidamente a los incidentes. Puede configurar Amazon CloudWatch y Amazon EventBridge para crear automáticamente incidentes basados en alarmas de CloudWatch y eventos de EventBridge. También puede crear incidentes manualmente en la página de la lista de incidentes o utilizando la acción de la API [StartIncident](#) del SDK de la AWS CLI o de AWS. Incident Manager deduplica los incidentes creados a partir de la misma alarma de CloudWatch o evento de EventBridge en el mismo incidente.

Para incidentes creados automáticamente por alarmas de CloudWatch o eventos de EventBridge, Incident Manager intenta crear un incidente en la misma Región de AWS que la regla o alarma del evento. En el caso de que Incident Manager no esté disponible en la Región de AWS, CloudWatch o EventBridge crearán automáticamente el incidente en una de las regiones disponibles especificadas en su conjunto de réplica. Para obtener más información, consulte [Administración de incidentes entre regiones y entre cuentas en Incident Manager](#).

Cuando el sistema crea un incidente, Incident Manager recopila automáticamente información sobre los recursos de AWS implicados en el incidente y añade esta información a la pestaña Elementos relacionados. Si ha especificado un manual de procedimientos en su plan de respuesta, cuando el sistema crea un incidente, Incident Manager puede enviar la información sobre los recursos de AWS implicados en el incidente al manual de procedimientos. El sistema puede entonces apuntar a esos recursos cuando inicie el manual de procedimientos e intente corregir el problema.

Cuando el sistema crea un incidente, también crea un elemento de trabajo operativo matriz (OpsItem) en OpsCenter, un componente de Systems Manager, y lo vincula al incidente como elemento relacionado. Puede utilizar este OpsItem para realizar un seguimiento del trabajo relacionado y futuros análisis de incidentes. Las llamadas al OpsCenter conllevan costos. Para obtener más información sobre los precios de OpsCenter, consulte [Precios de Systems Manager](#).

Important

Tenga en cuenta los siguientes detalles importantes.

- En el caso de que Incident Manager no esté disponible, el sistema solo puede conmutar por error y crear incidentes en otras Regiones de AWS si ha especificado al menos dos regiones en su conjunto de réplica. Para obtener información sobre la configuración de un conjunto de réplica, consulte [Introducción a Incident Manager](#).

- Los incidentes creados por una conmutación por error entre regiones no invocan los manuales de procedimientos especificados en los planes de respuesta.

Creación automática de incidentes con alarmas de CloudWatch

CloudWatch utiliza sus métricas de CloudWatch para alertarle sobre cambios en su entorno y realizar automáticamente la acción de iniciar incidente. CloudWatch trabaja con Systems Manager e Incident Manager para crear un incidente a partir de una plantilla de plan de respuesta cuando una alarma pasa al estado de alarma. Esto requiere los siguientes requisitos previos:

- Incident Manager configurado y conjunto de réplica creado. Este paso crea el rol vinculado al servicio de Incident Manager en su cuenta, proporcionando los permisos necesarios.
- Plan de respuesta de Incident Manager configurado. Para obtener información sobre cómo configurar los planes de respuesta de Incident Manager, consulte [Uso de los planes de respuesta en Incident Manager](#) en la sección Preparación de incidentes de esta guía.
- Métricas CloudWatch configuradas que monitoreen su aplicación. Para conocer las prácticas recomendadas de monitoreo, consulte [Supervisión](#) en la sección Preparación de incidentes de esta guía.

Para crear una alarma con una acción Iniciar incidente

1. Cree una alarma en CloudWatch. Para obtener más información, consulte [Uso de las alarmas de Amazon CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.
2. Al elegir la acción que debe realizar la alarma, seleccione Añadir acción de Systems Manager.
3. Elija Crear incidente y seleccione el Plan de respuesta para este incidente.
4. Complete los pasos restantes de la guía del tipo de alarma seleccionada.

Tip

También puede añadir la acción de crear incidente a cualquier alarma existente.

Creación automática de incidentes con eventos de EventBridge

Las reglas de EventBridge observan patrones de eventos. Si el evento coincide con el patrón definido, Incident Manager crea un incidente utilizando el plan de respuesta elegido.

Creación de incidentes mediante eventos de socios SaaS

Puede configurar EventBridge para recibir eventos de aplicaciones y servicios de socios de software como servicio (SaaS), lo que permite la integración de terceros. Después de configurar EventBridge para recibir eventos de socios de terceros, puede crear reglas que coincidan con los eventos de socios para crear incidentes. Para ver una lista de integraciones de terceros, consulte [Recepción de eventos de un socio SaaS](#).

Configure EventBridge para recibir eventos de una integración SaaS.

1. Abra la consola de Amazon EventBridge en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, elija Partner event sources (Orígenes de eventos de socios).
3. Utilice la barra de búsqueda para encontrar el socio que desee y elija Configurar para ese socio.
4. Elija Copy (Copiar) para copiar su ID de cuenta en el portapapeles.

Note

Para la integración con Salesforce, siga los pasos descritos en la [Guía del usuario de Amazon AppFlow](#).

5. Vaya al sitio web del socio y siga las instrucciones para crear un origen de eventos de socio. Utilice su ID de cuenta para esto. El origen de eventos que cree estará disponible solo en su cuenta.
6. Vuelva a la consola de EventBridge y elija Orígenes de eventos de socios en el panel de navegación.
7. Seleccione el botón situado junto al origen de eventos de socios y elija Associate with event bus (Asociar con bus de eventos).

Creación de una regla que se active en los eventos de un socio SaaS

1. Abra la consola de Amazon EventBridge en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, seleccione Rules.


3. Elija Create rule.
4. Escriba un nombre y una descripción de la regla.

Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

5. En Bus de eventos, elija el bus de eventos que corresponda a este socio.
6. En Rule type (Tipo de regla), elija Rule with an event pattern (Regla con un patrón de evento).
7. Elija Siguiente.
8. En Event source (Origen del evento), elija AWS events or EventBridge partner events (Eventos o eventos de socios de EventBridge).
9. En Patrón del evento, elija Formulario de patrón de eventos.
10. En Origen del evento, elija Socios de EventBridge.
11. En Socios, elija el nombre del socio.
12. En Event type (Tipo de evento), elija All Events (Todos los eventos) o elija el tipo de evento que desea utilizar para esta regla. Si elige All Events (Todos los eventos), todos los eventos emitidos por este origen de eventos de socio coincidirán con la regla.

Si desea personalizar el patrón del evento, elija Editar, realice los cambios y, a continuación, elija Guardar.

13. Elija Siguiente.
14. En Seleccionar un objetivo, elija Plan de respuesta de Incident Manager y, a continuación, elija un Plan de respuesta.

 Note

Al seleccionar un plan de respuesta, todos los planes de respuesta que posea y hayan sido compartidos con su cuenta aparecerán en la lista desplegable Plan de respuesta.

15. EventBridge puede crear el rol de IAM necesario para que se ejecute su regla:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente).
16. Elija Siguiente.

17. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulte [Amazon EventBridge tags](#) (Etiquetas de Amazon EventBridge) en la Guía del usuario de Amazon EventBridge.
18. Elija Siguiente.
19. Revise su regla y, a continuación, elija Crear regla.

Creación de incidentes mediante eventos de servicios de AWS

EventBridge también recibe eventos de los servicios de AWS enumerados en [Eventos de servicios de AWS admitidos](#). De forma similar a cómo se configuran las reglas para los socios SaaS, puede configurarlas para los servicios de AWS.

Creación de una regla que se active ante eventos de un servicio de AWS


1. Abra la consola de Amazon EventBridge en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, seleccione Rules.
3. Elija Create rule.
4. Escriba un nombre y una descripción de la regla.

Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

5. En Event bus (Bus de eventos), elija Default (Predeterminado).
6. En Rule type (Tipo de regla), elija Rule with an event pattern (Regla con un patrón de evento).
7. Elija Siguiente.
8. En Event source (Origen del evento), elija AWS events or EventBridge partner events (Eventos o eventos de socios de EventBridge).
9. En Patrón del evento, elija Formulario de patrón de eventos.
10. En Event source (Origen del evento), elija AWS services (Servicios de).
11. En Nombre del servicio, elija el servicio que monitorea un incidente.
12. En Event type (Tipo de evento), elija All Events (Todos los eventos) o elija el tipo de evento que desea utilizar para esta regla. Si elige All Events (Todos los eventos), todos los eventos emitidos por este origen de eventos de socio coincidirán con la regla.

Si desea personalizar el patrón del evento, elija Editar, realice los cambios y, a continuación, elija Guardar.

13. Elija Siguiente.
14. En Seleccionar un objetivo, elija Plan de respuesta de Incident Manager y, a continuación, elija un Plan de respuesta.

 Note

Al seleccionar un plan de respuesta, todos los planes de respuesta que posea y hayan sido compartidos con su cuenta aparecerán en la lista desplegable Plan de respuesta.

15. EventBridge puede crear el rol de IAM necesario para que se ejecute su regla:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente).
16. Elija Siguiente.
17. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulte [Amazon EventBridge tags](#) (Etiquetas de Amazon EventBridge) en la Guía del usuario de Amazon EventBridge.
18. Elija Siguiente.
19. Revise su regla y, a continuación, elija Crear regla.

Creación manual de incidentes

Los respondedores pueden realizar un seguimiento manual de un incidente mediante la consola de Incident Manager a través de un plan de respuesta predefinido. Efectúe los siguientes pasos para crear un incidente.

1. Abra la [consola de Incident Manager](#).
2. Elija Iniciar incidente.
3. En Plan de respuesta, elija un plan de respuesta en la lista.
4. (Opcional) Para anular el título proporcionado por el plan de respuesta definido, introduzca un Título del incidente.
5. (Opcional) Para anular el impacto proporcionado por el plan de respuesta definido, introduzca el Impacto del incidente.

Seguimiento de incidentes en Incident Manager

AWS Systems Manager Incident Manager realiza el seguimiento de los incidentes desde el momento en que se detectan hasta su resolución y a través del análisis post-incidente. Puede encontrar todos los incidentes en la página Lista de incidentes de la consola de Incident Manager, con enlaces directos a los Detalles del incidente.

Temas

- [Lista de incidentes](#)
- [Detalles del incidente](#)

Lista de incidentes

La página Lista de incidentes contiene tres secciones: Incidentes abiertos, Incidentes resueltos y Análisis. Puede hacer un seguimiento manual de los nuevos incidentes y crear análisis desde esta página. Para obtener más información sobre el seguimiento manual de un incidente, consulte [Creación manual de incidentes](#) en la sección Creación de incidentes de esta guía. Para obtener información sobre el análisis post-incidente, consulte la sección [Realización de un análisis post-incidente en Incident Manager](#) de esta guía.

Detalles del incidente muestra los Incidentes abiertos en mosaicos con el título, el impacto, la duración y el canal de chat de ese incidente. Después de resolver un incidente, este pasa a la lista Incidentes resueltos. Los Análisis se encuentran en la segunda pestaña.

Detalles del incidente

La página Detalles del incidente proporciona información detallada y herramientas que puede utilizar para administrar un incidente. Desde esta página, puede iniciar manuales de procedimientos para mitigar un incidente, añadir notas sobre el mismo, involucrar a otros solucionadores y ver detalles del incidente como líneas temporales, métricas, propiedades y recursos relacionados. La página Detalles del incidente incluye las siguientes secciones: Banner superior, Notas del incidente y siete pestañas que contienen información y recursos adicionales. De forma predeterminada, las secciones Banner superior y Notas del incidente se muestran en toda la página Detalles del incidente.

En este tema se explican los elementos de la página Detalles del incidente y las acciones que puede realizar desde la misma.

Banner superior

El banner superior de cada página de detalles del incidente incluye la siguiente información:

- Estado: el estado actual de un incidente, que puede ser Abierto o Resuelto.
- Impacto: el impacto del incidente en su entorno. Puede ser alto, medio y bajo. Para cambiar el impacto de un incidente, elija Editar propiedades.
- Canal de chat: un enlace para acceder al canal de chat donde puede ver las actualizaciones y notificaciones de incidentes.
- Duración: el tiempo transcurrido antes de que un respondedor resuelva el incidente.
- Manuales de procedimientos: los estados de los manuales de procedimientos asociados a este incidente. El estado puede ser esperando entrada, exitoso, o fallido. Si el estado de un manual de procedimientos es esperando entrada, puede seleccionar el manual de procedimientos para ver los detalles de la acción. Puede seleccionar fallido para ver los manuales de procedimientos que estén en estado Vencido, Fallido o Cancelado.
- Participaciones: el número total de participaciones y el estado de cada una de ellas. Al crear una participación, su estado es Participante. Una vez que reconoce la participación, el estado cambia de Participante a Reconocido. Incident Manager no admite el reconocimiento de participantes terceros. Dichos participantes permanecen en el estado Participante.

Para editar el título del incidente, el impacto y el canal de chat, elija Editar en la esquina superior derecha del banner.

Notas del incidente

La parte derecha de la pantalla muestra la sección Notas del incidente. Con las notas, puede colaborar y comunicar con otros usuarios que trabajen en un incidente. Puede explicar las mitigaciones que aplicó, una posible causa raíz que identificó o el estado actual del incidente. Como práctica recomendada, utilice la sección Notas del incidente para publicar actualizaciones de estado y acciones que usted u otras personas efectúen en un incidente. Si necesita comunicar con otros solucionadores en tiempo real, utilice el canal de chat disponible en Incident Manager.

Para añadir una nota, pulse el botón Añadir nota del incidente y, a continuación, introduzca su nota. Las notas pueden contener actualizaciones sobre el estado del incidente o cualquier otra información relevante que proporcione visibilidad a otros usuarios. De ser necesario, también puede editar o eliminar notas de incidentes.

Note

Cualquier usuario con permiso de IAM para ejecutar las acciones `ssm-incidents:UpdateTimelineEvent` y `ssm-incidents>DeleteTimelineEvent` puede editar y eliminar notas. Sin embargo, al compartir un incidente con otra cuenta, la política de recursos no incluye la acción `ssm-incidents>DeleteTimelineEvent`. Esto impide que el usuario con el que comparte el incidente elimine la nota. Puede ver el registro de auditoría de una nota de incidentes de Incident Manager en la consola de AWS CloudTrail.

Pestañas

La página de detalles del incidente tiene siete pestañas, lo que facilita a los respondedores la localización y visualización de la información durante un incidente. Las pestañas muestran un contador en el nombre de la pestaña, que indica el número de actualizaciones de la misma. Para obtener más información sobre el contenido de cada pestaña, así como sobre las acciones disponibles, prosiga con la lectura.

Información general

La pestaña Resumen es la página de aterrizaje para los respondedores. Contiene el resumen del incidente, una lista de eventos recientes de la línea temporal y el paso actual del manual de procedimientos.

Los respondedores utilizan el Resumen para ponerse al día sobre las acciones que se han realizado, los resultados de cualquier cambio, los posibles pasos siguientes e información sobre el impacto del incidente. Para actualizar el resumen, seleccione Editar en la esquina superior derecha de la sección Resumen.

Important

Si varios respondedores editasen el campo de resumen simultáneamente, el respondedor que envíe sus ediciones en último lugar sobrescribirá todas las demás entradas.

La sección Eventos recientes en la línea temporal contiene una línea temporal rellena por Incident Manager con los cinco eventos más recientes. Utilice esta sección para conocer el estado del incidente y lo que ha ocurrido recientemente. Para ver una línea temporal completa, prosiga en la pestaña Línea temporal.

La página de resumen también muestra el Paso actual del manual de procedimientos. Este paso puede ser un paso automático que se ejecuta en su entorno de AWS o un conjunto de instrucciones manuales para los respondedores. Para ver el manual de procedimientos completo, incluyendo los pasos anteriores y futuros, seleccione la pestaña Manual de procedimientos.

Diagnóstico

La pestaña Diagnóstico contiene información vital sobre sus sistemas y aplicaciones alojadas en AWS, incluyendo información sobre métricas y, si están habilitados, resultados.

Uso de métricas

Incident Manager utiliza Amazon CloudWatch para rellenar los gráficos de métricas y alarmas que se encuentran en esta pestaña. Para obtener más información sobre las prácticas recomendadas de administración de incidentes para definir alarmas y métricas, consulte [Supervisión](#) en la sección Planificación de incidentes de esta guía del usuario.

Para añadir métricas

- Seleccione Añadir en la esquina superior derecha de esta pestaña.
 - Para añadir una métrica desde un panel de control de CloudWatch existente, elija Desde panel de control de CloudWatch existente.
 - a. Elija un Panel de control. Esto añade todas las métricas y alarmas que forman parte del panel de control elegido.
 - b. (Opcional) También puede Seleccionar métricas desde el panel de control para ver métricas específicas.
 - Para añadir una única métrica, elija Desde CloudWatch y pegue un origen de métrica. Para copiar un origen de métrica
 - a. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
 - b. En el panel de navegación, seleccione Metrics (Métricas).
 - c. En la pestaña Todas las métricas, introduzca un término de búsqueda en el campo de búsqueda, como el nombre de una métrica o el nombre de un recurso, y elija Intro.

Por ejemplo, si busca la métrica CPUUtilization, verá los espacios de nombres y dimensiones asociados a esta métrica.
 - d. Elija uno de los resultados de su búsqueda para ver las métricas.
 - e. Elija la pestaña Origen y copie el origen.

Los gráficos de alarma de las métricas solo se pueden añadir a los detalles del incidente a través del plan de respuesta relacionado, o al seleccionar Desde el panel de control existente de CloudWatch al añadir una métrica.

Para eliminar métricas, seleccione Eliminar y, a continuación, elija las métricas que desee eliminar en el cuadro desplegable Métricas proporcionado.

Visualización de resultados desde AWS CodeDeploy y AWS CloudFormation

Una vez habilitados los resultados y configurados todos los permisos necesarios, los resultados que puedan estar relacionados con un incidente en concreto se vincularán al mismo. Los respondedores pueden ver información sobre estos resultados en la página Detalles del incidente.

Para ver los resultados desde CodeDeploy y CloudFormation

1. Abra la [consola de Incident Manager](#).
2. Elija el nombre de un incidente que desee investigar.
3. En la pestaña Diagnóstico, en el área Resultados, compare las horas de inicio de cualquier resultado notificado con la hora de inicio del incidente.
4. Para ver más detalles sobre un resultado, en la columna Referencia, elija el enlace al resultado de CodeDeploy o CloudFormation.

Plazo

Utilice la pestaña Línea temporal para realizar un seguimiento de los eventos que se producen durante un incidente. Incident Manager rellena automáticamente los eventos de la línea temporal que identifican sucesos significativos durante el incidente. Los respondedores pueden añadir eventos personalizados basados en sucesos detectados manualmente. Durante el análisis post-incidente, la pestaña de línea temporal proporciona información valiosa sobre cómo prepararse y responder mejor a los incidentes en el futuro. Para obtener más información sobre el análisis post-incidente, consulte [Realización de un análisis post-incidente en Incident Manager](#).

Para añadir un evento de línea temporal personalizado, seleccione Añadir. Seleccione una fecha utilizando el calendario y, a continuación, introduzca una hora. Todas las horas se muestran en su zona horaria local. Proporcione una breve descripción del evento que aparece en la línea temporal.

Para editar un evento personalizado existente, seleccione el evento en la línea temporal y elija Editar. Puede cambiar la hora, fecha y descripción de los eventos personalizados. Solo puede editar eventos personalizados.

Manuales de procedimientos

La pestaña Manuales de procedimientos de la página de detalles del incidente es donde los respondedores pueden ver los pasos del manual de procedimientos e iniciar nuevos manuales.

Para iniciar un nuevo manual de procedimientos, seleccione Iniciar manual de procedimientos en la sección Manuales de procedimientos. Utilice el campo de búsqueda para encontrar el manual de procedimientos que desea iniciar. Proporcione los Parámetros necesarios y la Versión del manual de procedimientos que desea utilizar al iniciar el manual. Los manuales de procedimientos iniciados durante un incidente desde la pestaña Manuales de procedimientos utilizan los permisos de la cuenta actualmente en sesión iniciada.

Para acceder a la definición de un manual de procedimientos en Systems Manager, seleccione el título del mismo en Manuales de procedimientos. Para navegar hasta la instancia en ejecución del manual de procedimientos en Systems Manager, elija los detalles de la ejecución en Detalles de la ejecución. Estas páginas muestran la plantilla utilizada para iniciar el manual de procedimientos y los detalles específicos de la instancia en ejecución del documento de automatización.

La sección Pasos del manual de procedimientos muestra la lista de pasos que el manual de procedimientos seleccionado realiza automáticamente o que los respondedores realizan manualmente. Los pasos se expanden a medida que se convierten en el paso actual, mostrando la información necesaria para completar el paso o detalles sobre lo que hace el paso. Los pasos automáticos del manual de procedimientos se resuelven una vez completada la automatización. Los pasos manuales requieren que los respondedores elijan Paso siguiente en la parte inferior de cada paso. Una vez completado un paso, la salida del paso aparece como un cuadro desplegable.

Para cancelar la ejecución de un manual de procedimientos, elija Cancelar manual de procedimientos. Esto detiene la ejecución del manual de procedimientos y no se completa ningún paso más en el mismo.

Participaciones

La pestaña Participaciones en detalles del incidente controla la participación de los respondedores y los equipos. Desde esta pestaña puede ver a quién se ha contactado, quién ha respondido, así como qué respondedores se van a involucrar como parte de un plan de escalada. Los respondedores pueden comprometer a otros contactos directamente desde esta pestaña. Para obtener más información sobre creación de contactos y planes de escalada, consulte las secciones [Uso de los contactos en Incident Manager](#) y [Uso de los planes de escalada en Incident Manager](#) de esta guía.

Puede configurar planes de respuesta con contactos y planes de escalada para iniciar automáticamente la participación al principio de un incidente. Para obtener más información sobre la configuración de planes de respuesta, consulte la sección [Uso de los planes de respuesta en Incident Manager](#) de esta guía.

Puede encontrar información sobre cada contacto en la tabla. Esta tabla incluye la siguiente información:

- Nombre: enlaces a la página de detalles del contacto que muestra sus métodos de contacto y su plan de participación.
- Plan de escalada: enlaces al plan de escalada que involucró al contacto.

- Origen del contacto: identifica el servicio que involucró a este contacto, como AWS Systems Manager o PagerDuty.
- Participante: muestra cuándo el plan involucró a un contacto, o cuándo involucrar a un contacto como parte de un plan de escalada.
- Reconocido: muestra si el contacto ha reconocido la participación.

Para confirmar una participación, el respondedor puede realizar una de las siguientes acciones:

- Llamada telefónica: Introduzca **1** cuando se le solicite.
- SMS: responda al mensaje con el código proporcionado o introdúzcalo en la pestaña Participaciones del incidente.
- Correo electrónico: introduzca el código proporcionado en la pestaña Participaciones del incidente.

Elementos relacionados

La pestaña Elementos relacionados se utiliza para recopilar recursos relacionados con la mitigación de incidentes. Estos recursos pueden ser ARN, enlaces a recursos externos o archivos cargados en buckets de Amazon S3. La tabla muestra un título descriptivo y un ARN, un enlace o detalles del bucket. Antes de utilizar los buckets de S3, consulte [Prácticas recomendadas de seguridad de Amazon S3](#) en la Guía del usuario de Amazon S3.

Al cargar archivos en un bucket de Amazon S3, el control de versiones podría estar habilitado o suspendido en dicho bucket. Cuando el control de versiones está habilitado en el bucket, los archivos subidos con el mismo nombre que un archivo existente se añaden como nueva versión del archivo. Si el control de versiones está suspendido, los archivos subidos con el mismo nombre que un archivo existente sobrescriben el archivo existente. Para obtener más información sobre el control de versiones, consulte [Uso del control de versiones en los buckets de S3](#) en la Guía del usuario de Amazon S3.

Al eliminar un elemento relacionado con un archivo, el archivo se elimina de la incidencia pero no se elimina del bucket de Amazon S3. Para obtener más información sobre cómo eliminar objetos de un bucket de Amazon S3, consulte [Eliminación de objetos de Amazon S3](#) en la Guía del usuario de Amazon S3.

Propiedades

La pestaña Propiedades proporciona los siguientes detalles sobre el incidente.

En la sección Propiedades del incidente, puede ver lo siguiente:

- Estado: describe el estado actual del incidente. El incidente puede estar Abierto o Resuelto.
- Hora de inicio: la hora en que se creó el incidente en Incident Manager.
- Hora de resolución: la hora en que se resolvió el incidente en Incident Manager.
- Nombre de recurso de Amazon (ARN): el ARN del incidente. Utilice el ARN cuando haga referencia al incidente desde el chat o con comandos de AWS Command Line Interface (AWS CLI).
- Plan de respuesta: identifica el plan de respuesta para el incidente seleccionado. Al seleccionar el plan de respuesta se abre la página de detalles del plan de respuesta.
- OpsItem matriz: identifica el OpsItem creado como matriz del incidente. Un OpsItem matriz puede tener múltiples incidentes relacionados y elementos de acción de seguimiento. Al seleccionar el OpsItem matriz se abre la página de detalles de OpsItems en OpsCenter.
- Análisis: identifica el análisis creado a partir de este incidente. Cree un análisis a partir de un incidente resuelto para mejorar su proceso de respuesta a incidentes. Seleccione el análisis para abrir la página de detalles del análisis.
- Propietario: la cuenta en la que se creó el incidente.

En la sección Etiquetas, puede ver y editar las claves y valores de las etiquetas asociadas al registro del incidente. Para obtener más información sobre las etiquetas en Incident Manager, consulte [Etiquetado de recursos en Incident Manager](#).

Realización de un análisis post-incidente en Incident Manager

El análisis post-incidente le guía en la identificación de mejoras en su respuesta a incidentes, incluyendo el tiempo de detección y mitigación. Un análisis también puede ayudarle a comprender la causa raíz de los incidentes. Incident Manager crea elementos de acción recomendados para mejorar su respuesta ante incidentes.

Beneficios de un análisis post-incidente

- Mejora de la respuesta ante incidentes
- Comprensión de la causa raíz del problema
- Afrontamiento de las causas raíz con elementos de acción factibles
- Análisis del impacto de los incidentes
- Captación y difusión de conocimientos dentro de una organización

Para qué no se debe utilizar un análisis

Un análisis es irreprochable y no llama a las personas por su nombre.

“Independientemente de lo que descubramos, entendemos y creemos de verdad que todo el mundo hizo el mejor trabajo posible, teniendo en cuenta lo que sabía en ese momento, sus habilidades y capacidades, los recursos disponibles y la situación en cuestión”. - Norm Kerth, Retrospectivas de proyectos: Un manual para la revisión en equipo

Detalles del análisis

La página de detalles del análisis le guía en la recopilación de información, la evaluación de mejoras y la creación de elementos de acción. La página de detalles del análisis es similar a la de detalles del incidente, pero tiene algunas diferencias clave, como las métricas históricas, la línea temporal editable y las preguntas para mejorar futuros incidentes.

Información general

Información general es un resumen del incidente. Este resumen incluye los antecedentes, lo que ocurrió, por qué ocurrió, cómo se mitigó, la duración y los elementos de acción clave para evitar que

el incidente vuelva a ocurrir. La información general es de alto nivel. Puede explorar más detalles en la pestaña Preguntas del análisis.

Métricas

Utilice la pestaña de métricas para visualizar las métricas clave de su aplicación durante el periodo del incidente. Aquí puede añadir gráficos de métricas que tengan una o más métricas representadas en el mismo gráfico. Las métricas utilizadas durante un incidente se rellenan automáticamente en esta pestaña. Le recomendamos que añada una descripción, un título y anotaciones de los puntos temporales clave durante el incidente.

Algunos puntos temporales clave que puede tener en cuenta al analizar un gráfico de métricas:

- Cambio de implementación
- Cambio de configuración
- Hora de inicio del incidente
- Hora de la alarma
- Hora de intervención
- Hora de inicio de la mitigación
- Hora de resolución del incidente

Limitaciones

- Las alarmas y expresiones de métricas de CloudWatch no se importan desde un incidente.
- Las métricas que se encuentren en una región que Incident Manager no admita no se importan desde el incidente.
- Las métricas en cuentas de la aplicación requieren la configuración del `CloudWatch-CrossAccountSharingRole` antes de crear el análisis. Para obtener más información sobre el rol, consulte [Consola multicuenta y multirregión de CloudWatch](#) en la guía del usuario de CloudWatch.

Plazo

Describa los puntos temporales clave en la línea temporal a medida que profundiza en la comprensión del incidente. La línea temporal de los incidentes se rellena automáticamente en esta

pestaña. Puede eliminar los puntos temporales que no sean relevantes para el análisis. También puede añadir y editar puntos temporales para describir con mayor precisión el incidente y su impacto.

Utilice la pestaña de línea temporal para responder a las preguntas que encuentre en la pestaña Preguntas sobre la respuesta al incidente.

Preguntas

Utilice las preguntas de Incident Manager para mejorar el tiempo de resolución de incidentes en su aplicación y reducir la aparición de incidentes. A medida que responda a las preguntas, actualice las pestañas Métricas y Línea temporal para mejorar su exactitud. Las preguntas se centran en estos aspectos clave de la respuesta ante incidentes:

- **Detección:** ¿Podría mejorar el tiempo de detección? ¿Existen actualizaciones de las métricas y alarmas que detectarían el incidente en menos tiempo?
- **Diagnóstico:** ¿Puede mejorar el tiempo previo al diagnóstico? ¿Existen actualizaciones para sus planes de respuesta o planes de escalada que implicarían en menos tiempo a los respondedores correctos?
- **Mitigación:** ¿Puede mejorar el tiempo previo a la mitigación? ¿Hay pasos del manual de procedimientos que podría añadir o mejorar?
- **Prevención:** ¿Puede evitar que se produzcan futuros incidentes? Para descubrir las causas fundamentales de un incidente, Amazon utiliza el enfoque de los 5 porqués en la investigación de problemas.

Acciones

Incident Manager crea elementos de acción recomendados para que los revise a medida que completa las preguntas. Puede elegir aceptar y completar estas acciones desde esta pestaña o puede descartarlas. Puede revisar los elementos de acción descartados; para ello, elija Elementos de acción descartados. Los elementos de acción son un tipo de OpsItem que están vinculados al análisis y al incidente en el OpsCenter.

Lista de comprobación

Antes de cerrar un análisis, utilice la lista de comprobación para revisar las acciones que un respondedor debería realizar. A medida que los respondedores completan las acciones de la lista de comprobación, el icono junto a la acción cambia de una elipse a una marca de verificación a

fin de indicar que la acción se ha completado. Si no ha completado los elementos de la lista de comprobación, Incident Manager muestra un mensaje para confirmar que el respondedor desea cerrar el análisis sin completarlo.

Plantillas de análisis

Una plantilla de análisis proporciona un conjunto de preguntas que profundizan en la causa raíz de los incidentes. Puede utilizar las respuestas a estas preguntas para mejorar el rendimiento de la aplicación y la respuesta a los incidentes.

Plantillas estándar de AWS

Incident Manager proporciona una plantilla estándar de preguntas basadas en las prácticas recomendadas de respuesta a incidentes y análisis de problemas de AWS llamada `AWSIncidents-PostIncidentAnalysisTemplate`.

Creación de una plantilla de análisis

Le sugerimos que utilice la plantilla de `AWSIncidents-PostIncidentAnalysisTemplate` predeterminada y añada preguntas o secciones adicionales que sean apropiadas para sus casos de uso. Cree plantillas de análisis basadas en la plantilla predeterminada. Utilice esta plantilla como punto de partida para crear plantillas de análisis en su cuenta de administrador. A continuación, puede duplicar sus plantillas de análisis en cada región en la que haya habilitado Incident Manager.

Creación de una plantilla de análisis

1. Invoque la acción `GetDocument` y utilice su parámetro `Name` para descargar `AWSIncidents-PostIncidentAnalysisTemplate`. Para obtener más información sobre la sintaxis de `GetDocument`, consulte [Referencia de la API de Systems Manager](#).
2. El contenido de la respuesta contiene los bloques de construcción JSON para el análisis. Utilice los bloques de construcción de preguntas para insertar preguntas adicionales en el análisis. Le recomendamos que añada preguntas o secciones en la sección `Incident questions`.
3. Para crear la nueva plantilla, utilice la operación `CreateDocument` con el JSON actualizado del paso anterior. Debe incluir lo siguiente, donde `Analysis_Template_Name` es el nombre de su plantilla,
 - `DocumentFormat: "JSON"`
 - `DocumentType: "ProblemAnalysisTemplate"`

- Name: "*Analysis_Template_Name*"

Creación de un análisis

1. Para crear un análisis, elija Crear análisis en la página de detalles del incidente de un incidente cerrado.
2. Elija la plantilla de análisis a partir de la cual crear este análisis e introduzca un nombre descriptivo del análisis.
3. Seleccione Crear.

Impresión de un análisis de incidente formateado

Puede generar una copia de un análisis completo o incompleto formateado para impresión. También puede guardar esta copia como archivo PDF. Puede imprimir un análisis cada vez. Actualmente no se admite la impresión por lotes de múltiples análisis.

Para imprimir un análisis formateado

1. Abra la [consola de Incident Manager](#).
2. Elija la pestaña Análisis.
3. Elija el título del análisis que desee imprimir.
4. En la esquina superior derecha de la página de detalles del análisis, elija Imprimir.
5. En el cuadro de diálogo Imprimir análisis de incidente, desactive las secciones del análisis que no desee incluir en la versión impresa. De forma predeterminada, están seleccionadas todas las secciones.
6. Elija Imprimir para abrir los controles de impresión locales de su dispositivo.
7. Elija el destino o formato de impresión. Puede elegir una impresora local o de red, o puede guardar el análisis en un archivo PDF. Realice cualquier cambio, si lo desea, en las opciones de impresión restantes y, a continuación, elija Imprimir.

Note

Controles de impresión locales se refiere a la interfaz de usuario proporcionada por su navegador web y dispositivo.

Destinos de impresión son aquellos configurados para su dispositivo y accesibles desde el mismo.

Tutoriales de Administración de incidentes

Estos tutoriales de AWS Systems Manager Incident Manager le ayudan a crear un sistema de gestión de incidentes más sólido. Estos tutoriales desarrollan actividades comunes llevadas a cabo durante un incidente o muestran cómo responder a determinados incidentes.

Temas

- [Uso de los manuales de procedimientos de Automatización de Systems Manager con Administración de incidentes](#)
- [Administración de incidentes de seguridad en Incident Manager](#)

Uso de los manuales de procedimientos de Automatización de Systems Manager con Administración de incidentes


Puede utilizar los manuales de [AWS Systems Manager automatización](#) para simplificar las tareas habituales de mantenimiento, implementación y corrección de los servicios. AWS En este tutorial, creará un manual de procedimientos personalizado para automatizar la respuesta a un incidente en Administración de incidentes. El escenario de este tutorial implica una CloudWatch alarma de Amazon asignada a una métrica de Amazon EC2. Cuando la instancia entra en un estado que activa la alarma, Administración de incidentes realiza automáticamente las siguientes tareas:

1. Crea un incidente en Administración de incidentes.
2. Inicia un manual de procedimientos que intenta corregir el problema.
3. Publica los resultados del manual de procedimientos en la página de detalles del incidente en Administración de incidentes.

El proceso descrito en este tutorial también se puede utilizar con EventBridge eventos de Amazon y otros tipos de AWS recursos. Al automatizar su respuesta de corrección a alarmas y eventos, puede reducir el impacto de un incidente en su organización y sus recursos.

En este tutorial se describe cómo editar una CloudWatch alarma asignada a una instancia de Amazon EC2 para un plan de respuesta de Incident Manager. Si no tiene una alarma, una instancia ni un plan de respuesta configurados, le recomendamos que configure esos recursos antes de comenzar. Para obtener más información, consulte los temas siguientes:

- [Uso de CloudWatch las alarmas de Amazon](#) en la Guía del CloudWatch usuario de Amazon
- [Instancias de Amazon EC2](#) en la Guía del usuario de Amazon EC2
- [Instancias de Amazon EC2](#) en la Guía del usuario de Amazon EC2
- [Uso de los planes de respuesta en Incident Manager](#)

 Important


La creación de AWS recursos y el uso de los pasos de automatización habituales generarán costes. Para más información, consulte [Precios de AWS](#).

Temas

- [Tarea 1: Creación del manual de procedimientos](#)
- [Tarea 2: Creación de un rol de IAM](#)
- [Tarea 3: Conexión del manual de procedimientos a su plan de respuesta](#)
- [Tarea 4: Asignar una CloudWatch alarma a su plan de respuesta](#)
- [Tarea 5: Verificación de resultados](#)

Tarea 1: Creación del manual de procedimientos

Utilice el siguiente procedimiento para crear un manual de procedimientos en la consola de Systems Manager. Cuando se invoca desde un incidente de Administración de incidentes, el manual de procedimientos reinicia una instancia de Amazon EC2 y actualiza el incidente con información sobre la ejecución del manual de procedimientos. Antes de comenzar, verifique que tiene permiso para crear un manual de procedimientos. Para obtener más información, consulte [Configuración de la automatización](#) en la Guía del usuario de AWS Systems Manager .

 Important

Revise los siguientes detalles importantes sobre la creación del manual de procedimientos de este tutorial:

- El manual está diseñado para un incidente creado a partir de una CloudWatch fuente de alarma. Si utiliza este manual de procedimientos para otro tipo de incidentes, por ejemplo,

incidentes creados manualmente, no se encontrará el evento de la línea temporal en el primer paso del manual de procedimientos y el sistema devolverá un error.

- El manual requiere que la CloudWatch alarma incluya una dimensión llamada InstanceId. Las alarmas para métricas de instancias de Amazon EC2 tienen esta dimensión. Si utiliza este manual con otras métricas (o con otras fuentes de incidentes, por ejemplo EventBridge), tendrá que cambiar el JsonDecode2 paso para que coincida con los datos capturados en su escenario.
- El manual de procedimientos intenta corregir el problema que activó la alarma reiniciando la instancia de Amazon EC2. En un incidente real, es posible que no desee reiniciar la instancia. Actualice el manual de procedimientos con las acciones de corrección específicas que desea que realice el sistema.

Para obtener más información sobre la creación de manuales de procedimientos, consulte [Trabajo con manuales de procedimientos](#) en la Guía del usuario de AWS Systems Manager .

Para crear un manual de procedimientos

1. Abra la AWS Systems Manager consola en <https://console.aws.amazon.com/systems-manager/>.
2. En el panel de navegación, elija Documentos.
3. Elija Automatización.
4. En Nombre, introduzca un nombre descriptivo para el manual de procedimientos, como **IncidentResponseRunbook**.
5. Elija la pestaña Editor y después elija Edit (Editar).
6. Pegue el siguiente contenido en el editor:

```
description: This runbook attempts to restart an Amazon EC2 instance that caused an
incident.
schemaVersion: '0.3'
parameters:
  IncidentRecordArn:
    type: String
    description: The incident
mainSteps:
  - name: ListTimelineEvents
    action: 'aws:executeAwsApi'
    outputs:
      - Selector: '$.eventSummaries[0].eventId'
```

```

    Name: eventId
    Type: String
  inputs:
    Service: ssm-incidents
    Api: ListTimelineEvents
    incidentRecordArn: '{{IncidentRecordArn}}'
    filters:
      - key: eventType
        condition:
          equals:
            stringValues:
              - SSM Incident Trigger
    description: This step retrieves the ID of the first timeline event with the
    CloudWatch alarm details.
  - name: GetTimelineEvent
    action: 'aws:executeAwsApi'
    inputs:
      Service: ssm-incidents
      Api: GetTimelineEvent
      incidentRecordArn: '{{IncidentRecordArn}}'
      eventId: '{{ListTimelineEvents.eventId}}'
    outputs:
      - Name: eventData
        Selector: $.event.eventData
        Type: String
    description: This step retrieves the timeline event itself.
  - name: JsonDecode
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
            data = json.loads(events["eventData"])
            return data
    InputPayload:
      eventData: '{{GetTimelineEvent.eventData}}'
    outputs:
      - Name: rawData
        Selector: $.Payload.rawData
        Type: String
    description: This step parses the timeline event data.

```

```

- name: JsonDecode2
  action: 'aws:executeScript'
  inputs:
    Runtime: python3.8
    Handler: script_handler
    Script: |-
      import json

      def script_handler(events, context):
        data = json.loads(events["rawData"])
        return data
  InputPayload:
    rawData: '{{JsonDecode.rawData}}'
  outputs:
    - Name: InstanceId
      Selector:
        '$.Payload.detail.configuration.metrics[0].metricStat.metric.dimensions.InstanceId'
      Type: String
    description: This step parses the CloudWatch event data.
- name: RestartInstance
  action: 'aws:executeAutomation'
  inputs:
    DocumentName: AWS-RestartEC2Instance
    DocumentVersion: $DEFAULT
    RuntimeParameters:
      InstanceId: '{{JsonDecode2.InstanceId}}'
  description: This step restarts the Amazon EC2 instance

```

7. Elija Create automation (Crear automatización).

Tarea 2: Creación de un rol de IAM

Utilice el siguiente tutorial para crear un rol AWS Identity and Access Management (de IAM) que dé permiso al administrador de incidentes para iniciar un manual especificado en un plan de respuesta. El manual de procedimientos de este tutorial reinicia una instancia de Amazon EC2. Especificará este rol de IAM en la siguiente tarea al conectar el manual de procedimientos a su plan de respuesta.

Creación de un rol de IAM que inicie un manual de procedimientos desde un plan de respuesta

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.

3. En Tipo de entidad de confianza, verifique que Servicio de AWS esté seleccionado.
4. En Caso de uso, en el campo Casos de uso para otros servicios de AWS , introduzca **Incident Manager**.
5. Elija Incident Manager y, a continuación, Siguiente.
6. En la página Añadir permisos, elija Crear política. El editor de permisos se abre en una nueva ventana o pestaña del navegador.
7. En el editor, elija la pestaña JSON.
8. Copie y pegue la siguiente política de permisos en el editor JSON. Sustituya *account_ID* por su ID de Cuenta de AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:ssm:*:account_ID:automation-definition/
IncidentResponseRunbook:*",
        "arn:aws:ssm:*::automation-definition/AWS-RestartEC2Instance:*"
      ],
      "Action": "ssm:StartAutomationExecution"
    },
    {
      "Effect": "Allow",
      "Resource": "arn:aws:ssm:*::automation-execution/*",
      "Action": "ssm:GetAutomationExecution"
    },
    {
      "Effect": "Allow",
      "Resource": "arn:aws:ssm-incidents:*:*:*",
      "Action": "ssm-incidents:*"
    },
    {
      "Effect": "Allow",
      "Resource": "arn:aws:iam:*::role/AWS-SystemsManager-
AutomationExecutionRole",
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Resource": "*",

```

```
        "Action": [  
            "ec2:StopInstances",  
            "ec2:DescribeInstanceStatus",  
            "ec2:StartInstances"  
        ]  
    }  
]  
}
```

9. Elija Siguiente: etiquetas.
10. (Opcional) De ser necesario, añada etiquetas a su política.
11. Elija Siguiente: Revisar.
12. En el campo Nombre, introduzca un nombre que le ayude a identificar este rol como utilizado para este tutorial.
13. (Opcional) Introduzca una descripción en el campo Descripción.
14. Elija Crear política.
15. Regrese a la ventana o pestaña del navegador correspondiente al rol que está creando. Se visualiza la página Añadir permisos.
16. Elija el botón de actualización (situado junto al botón Crear política) y, a continuación, introduzca el nombre de la política de permisos que ha creado en el cuadro de filtro.
17. Elija la política de permisos que ha creado y, a continuación, Siguiente.
18. En la página Nombre, revisión y creación, en Nombre del rol, introduzca un nombre que le ayude a identificar este rol como utilizado para este tutorial.
19. (Opcional) Introduzca una descripción en el campo Descripción.
20. Revise los detalles del rol, añada etiquetas si fuese necesario y seleccione Crear rol.

Tarea 3: Conexión del manual de procedimientos a su plan de respuesta

Al conectar el manual de procedimientos a su plan de respuesta de Administración de incidentes, se asegura un proceso de mitigación coherente, repetible y oportuno. El manual de procedimientos también sirve como punto de partida para que los solucionadores determinen su siguiente curso de acción.

Para asignar el manual de procedimientos a su plan de respuesta

1. Abra la [consola de Administración de incidentes](#).

2. Elija Planes de respuesta.
3. En Plan de respuesta, elija un plan de respuesta existente y seleccione Editar. Si no tiene un plan de respuesta existente, elija Crear plan de respuesta para crear uno nuevo.

Complete los siguientes campos:

- a. En la sección Manual de procedimientos, elija Seleccionar manual de procedimientos existente.
 - b. En Propietario, compruebe que Propiedad mía esté seleccionado.
 - c. En Manual de procedimientos, seleccione el manual de procedimientos que creó en [Tarea 1: Creación del manual de procedimientos](#).
 - d. En Versión, elija Predeterminado en el momento de ejecución.
 - e. En la sección Entradas, para el parámetro IncidentRecordArn, elija ARN de incidente.
 - f. En la sección Permisos de ejecución, elija el rol de IAM que creó en [Tarea 2: Creación de un rol de IAM](#).
4. Guarde los cambios.

Tarea 4: Asignar una CloudWatch alarma a su plan de respuesta

Utilice el siguiente procedimiento para asignar una CloudWatch alarma para una instancia de Amazon EC2 a su plan de respuesta.

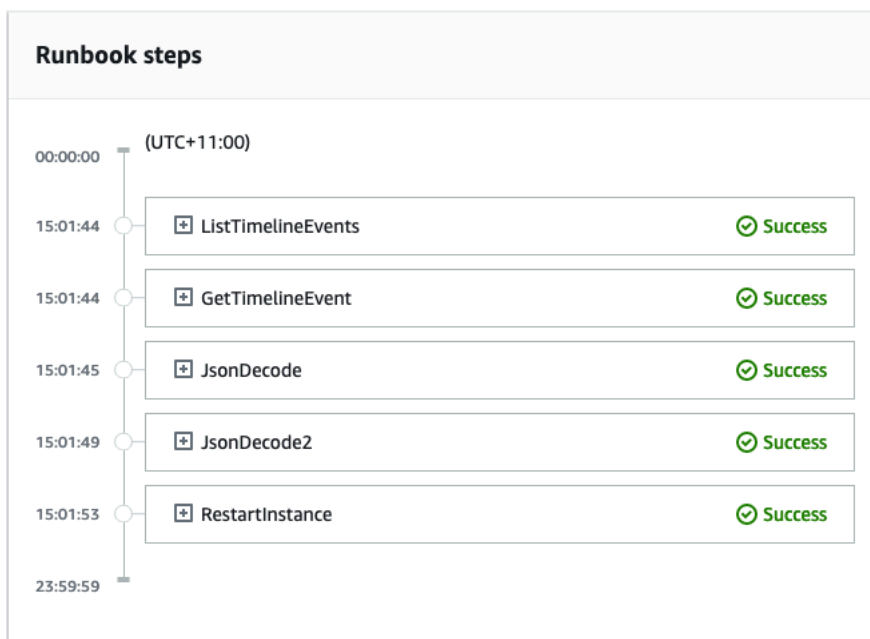
Para asignar una CloudWatch alarma a su plan de respuesta

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, en Alarmas, elija Todas las alarmas.
3. Elija una alarma para una instancia de Amazon EC2 que desee conectar a su plan de respuesta.
4. Seleccione Acciones y, a continuación, Editar. Compruebe que la métrica tenga una dimensión denominada InstanceId.
5. Elija Siguiente.
6. En Asistente para configurar acciones, elija Añadir acción de Systems Manager.
7. Elija Crear incidente.
8. Elija el plan de respuesta que creó en [Tarea 3: Conexión del manual de procedimientos a su plan de respuesta](#).
9. Elija Update alarm (Actualizar alarma).

Tarea 5: Verificación de resultados

Para comprobar que la CloudWatch alarma crea un incidente y, a continuación, procesa el manual especificado en su plan de respuesta, debe activar la alarma. Tras activar la alarma y una vez que finalice el procesamiento del manual de procedimientos, puede verificar los resultados del manual de procedimientos mediante el siguiente procedimiento. Para obtener más información sobre la activación de una alarma, consulte [set-alarm-state](#) en la Referencia de comandos de AWS CLI .

1. Abra la [consola de Administración de incidentes](#).
2. Elija el incidente creado por la CloudWatch alarma.
3. Elija la pestaña Manuales de procedimientos.
4. Vea las acciones realizadas en su instancia de Amazon EC2 en la sección Pasos del manual de procedimientos. La siguiente imagen es un ejemplo que muestra los pasos realizados por el manual de procedimientos que ha creado en este tutorial. Cada paso se enumera con una marca de tiempo y un mensaje de estado.



Para ver todos los detalles de la CloudWatch alarma, expanda los JsonDecodedos pasos y, a continuación, expanda la opción Salida.

Important

Debe sanear cualquier cambio en los recursos que haya implementado durante este tutorial y que no desee conservar. Esto incluye cambios en los recursos del administrador de

incidentes, como los planes de recursos y los incidentes, los cambios en CloudWatch las alarmas y la función de IAM que creó para este tutorial.

Administración de incidentes de seguridad en Incident Manager

Puede usar AWS Security Hub Amazon EventBridge e Incident Manager juntos para identificar y gestionar los incidentes de seguridad en sus aplicaciones AWS alojadas. En este tutorial, se explica cómo configurar una EventBridge regla que cree un incidente en función de las conclusiones enviadas automáticamente por Security Hub.

Note

En este tutorial se utiliza EventBridge Security Hub. Podría incurrir en costos por el uso de estos servicios.

Requisitos previos

- Configure Security Hub. Para más información, consulte [Configuración AWS Security Hub](#).
- Cree o actualice los resultados en Security Hub. Para obtener más información, consulte [Resultados en AWS Security Hub](#).
- Configure un plan de respuesta que Incident Manager utilice como plantilla al crear su incidente de seguridad. Para obtener más información, consulte [Preparación para incidentes en Incident Manager](#).

En este tutorial, utilizamos un patrón predefinido para crear la EventBridge regla. Para crear la regla con un patrón personalizado, consulte [Uso de un patrón personalizado para crear la regla](#) en la guía del AWS Security Hub usuario.

Cree una EventBridge regla

1. Abra la EventBridge consola de Amazon en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, seleccione Reglas.
3. Elija Crear regla.
4. Escriba un nombre y la descripción de la regla.

Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

5. En Bus de eventos, elija Predeterminado.
6. En Tipo de regla, elija Regla con un patrón de evento.
7. Elija Siguiente.
8. En Fuente del evento, selecciona AWS eventos o eventos EventBridge asociados.
9. En Patrón del evento, elija Formulario de patrón de eventos.
10. En Origen del evento, seleccione Servicios de AWS .
11. En Servicio de AWS , elija Security Hub.
12. En Tipo de evento, elija Resultados de Security Hub - Importados.
13. De forma predeterminada, EventBridge configura el patrón de eventos sin ningún valor de filtro. Para cada atributo, se selecciona la opción Cualquier **nombre de atributo**. Actualice estos filtros para crear incidentes basados en los resultados de seguridad que más afecten a su entorno.
14. Haga clic en Next (Siguiente).
15. En Tipos de destino, seleccione Servicio de AWS .
16. En Seleccionar un objetivo, elija Plan de respuesta de Incident Manager.
17. En Plan de respuesta, elija un plan de respuesta para utilizarlo como plantilla para los incidentes creados.
18. EventBridge puede crear la función de IAM necesaria para que se ejecute la regla.
 - Para crear un rol de IAM de forma automática, elija Crear un nuevo rol para el recurso específico.
 - Para utilizar un rol de IAM que ya exista en su cuenta, elija Utilizar rol existente.
19. (Opcional) Introduzca una o varias etiquetas para la regla.
20. Seleccione Siguiente.
21. Revise los detalles de la regla y seleccione Crear regla.

Ahora que ha creado esta EventBridge regla, los fallos de seguridad que coincidan con los valores de los atributos que ha definido crearán incidentes en Incident Manager. Puede clasificar, administrar, monitorear y crear análisis post-incidente a partir de estos incidentes.

Etiquetado de recursos en Incident Manager

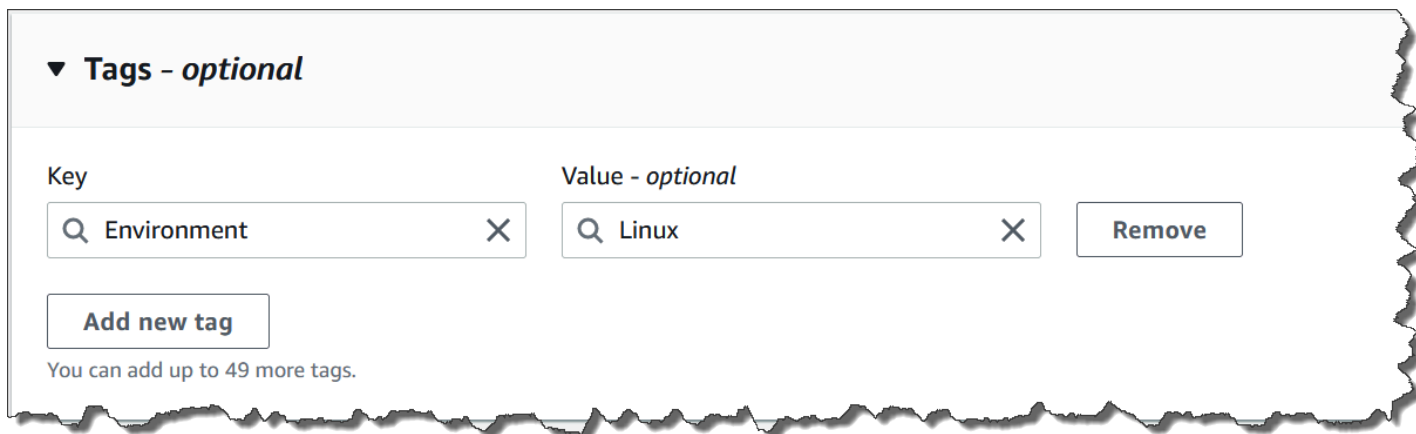
Las etiquetas son metadatos opcionales que puede asignar a sus recursos de Incident Manager en la Región de AWS especificada en su conjunto de réplica. Puede asignar etiquetas a planes de respuesta, registros de incidentes y contactos. También puede añadir etiquetas a los horarios y rotaciones de guardia. También puede añadir etiquetas al propio conjunto de réplica. Las etiquetas le permiten categorizar y controlar el acceso a estos recursos de diferentes maneras. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Le recomendamos que diseñe un conjunto de claves de etiquetas que satisfaga sus necesidades para cada tipo de recurso de Incident Manager. El uso de un conjunto coherente de claves de etiquetas le facilita la administración de estos recursos y el control del acceso a los mismos. Puede buscar y filtrar recursos en función de las etiquetas. Para obtener más información sobre el control del acceso a los recursos mediante el uso de etiquetas, consulte [Control del acceso a los recursos de AWS mediante etiquetas](#) en la Guía del usuario de IAM.

Puede especificar etiquetas en la sección Incidente predeterminado al crear un plan de respuesta. Estas etiquetas se aplican al registro del incidente cuando se crea un incidente utilizando el plan de respuesta.

Note


Las etiquetas no tienen ningún significado semántico. Se interpretan estrictamente como una cadena de caracteres.

Puede añadir o eliminar etiquetas mediante la consola de Incident Manager. La siguiente captura de pantalla muestra la sección de etiquetas al crear un nuevo plan de respuesta.



Para trabajar con etiquetas mediante programación, utilice las siguientes acciones de la API:

- [TagResource](#)
- [UntagResource](#)
- [ListTagsForResource](#)

 Important

Las etiquetas aplicadas a los planes de respuesta, los registros de incidentes, los contactos, los horarios y rotaciones de guardia y los conjuntos de réplica pueden verse y modificarse solo desde la cuenta del propietario del recurso.

Seguridad en AWS Systems Manager Incident Manager

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS programas](#) de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Systems Manager Incident Manager, consulte [AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar Incident Manager. En los siguientes temas le mostramos cómo configurar Incident Manager para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayuden a supervisar y proteger sus recursos de Incident Manager.

Temas

- [Protección de los datos en Incident Manager](#)
- [Identity and Access Management para AWS Systems Manager Incident Manager](#)
- [Uso compartido de contactos y planes de respuesta en Incident Manager](#)
- [Validación de conformidad para AWS Systems Manager Incident Manager](#)
- [Resiliencia en AWS Systems Manager Incident Manager](#)
- [Seguridad de la infraestructura en AWS Systems Manager Incident Manager](#)
- [Trabajar con VPC puntos finales AWS Systems Manager Incident Manager e interconectarse \(\)AWS PrivateLink](#)
- [Configuración y análisis de vulnerabilidades en Incident Manager](#)

- [Mejores prácticas de seguridad en AWS Systems Manager Incident Manager](#)

Protección de los datos en Incident Manager

El modelo de [responsabilidad AWS compartida modelo](#) se aplica a la protección de datos en AWS Systems Manager Incident Manager. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte la sección [Privacidad de datos FAQ](#). Para obtener información sobre la protección de datos en Europa, consulte el [modelo de responsabilidad AWS compartida](#) y la entrada del GDPR blog sobre AWS seguridad.

Para proteger los datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la [Norma federal de procesamiento de información \(\) FIPS 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Incident Manager u otro dispositivo Servicios de AWS mediante la consola, API AWS CLI, o. AWS SDKs Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros

de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

De forma predeterminada, Incident Manager cifra los datos en tránsito mediante SSL/TLS.

Cifrado de datos

Incident Manager utiliza las claves AWS Key Management Service (AWS KMS) para cifrar los recursos de Incident Manager. Para obtener más información al respecto AWS KMS, consulte la [Guía para AWS KMS desarrolladores](#). AWS KMS combina hardware y software seguros y de alta disponibilidad para proporcionar un sistema de administración de claves adaptado a la nube. Incident Manager cifra sus datos con la clave especificada y cifra los metadatos con una AWS clave propia. Para utilizar Incident Manager, debe configurar su conjunto de réplica, lo que incluye configurar el cifrado. Incident Manager requiere el cifrado de datos para su uso.

Puede utilizar una AWS clave propia para cifrar el conjunto de replicación o puede utilizar la clave gestionada por el cliente que creó AWS KMS para cifrar las regiones del conjunto de replicación. Incident Manager solo admite AWS KMS claves de cifrado simétricas para cifrar los datos creados en él. AWS KMS Incident Manager no admite AWS KMS claves con material de claves importado, almacenes de claves personalizados, códigos de autenticación de mensajes basados en hash (HMAC) ni ningún otro tipo de claves. Si usa claves administradas por el cliente, usa la [AWS KMS consola](#) o AWS KMS APIs para crear de forma centralizada las claves administradas por el cliente y definir las políticas clave que controlan cómo Incident Manager puede usar las claves administradas por el cliente. Cuando utiliza una clave gestionada por el cliente para el cifrado con Incident Manager, la clave gestionada por el AWS KMS cliente debe estar en la misma región que los recursos. Para obtener más información sobre cómo configurar el cifrado de datos en Incident Manager, consulte [Asistente de preparación](#).

El uso de claves administradas por el AWS KMS cliente conlleva cargos adicionales. Para obtener más información, consulte [AWS KMS Conceptos: KMS claves](#) en la Guía para AWS Key Management Service desarrolladores y [AWS KMS precios](#).

Important

Si utiliza una clave gestionada por el cliente (CMK) para cifrar el conjunto de replicación y los datos de Incident Manager, pero más adelante decide eliminarlo, asegúrese de eliminarlo antes de desactivarlo o eliminarlo. CMK

Para permitir que Incident Manager utilice su clave administrada por el cliente para cifrar sus datos, debe añadir las siguientes declaraciones de política a la política de claves de su clave administrada por el cliente. Para obtener más información sobre cómo configurar y cambiar la política de claves de su cuenta, consulte [Uso de políticas de claves en AWS KMS](#) en la Guía para desarrolladores de AWS Key Management Service . La política proporciona los siguientes permisos:

- Permite a Incident Manager realizar operaciones de solo lectura para encontrar la correspondiente a Incident Manager en CMK su cuenta.
- Permite a Incident Manager utilizarla CMK para crear subvenciones y describir la clave, pero solo cuando actúa en nombre de los directores de la cuenta que tienen permiso para usar Incident Manager. Si los responsables especificados en la declaración de política no tienen permiso para usar las KMS claves ni para usar Incident Manager, la llamada fallará, incluso si proviene del servicio Incident Manager.

```
{
  "Sid": "Allow CreateGrant through AWS Systems Manager Incident Manager",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ssm-lead"
  },
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "ssm-incidents.amazonaws.com",
        "ssm-contacts.amazonaws.com"
      ]
    }
  }
}
```

Sustituya el `Principal` valor por el IAM principal que creó el conjunto de replicación.

Incident Manager utiliza un [contexto de cifrado](#) en todas las AWS KMS solicitudes de operaciones criptográficas. Puede utilizar este contexto de cifrado para identificar los eventos de CloudTrail

registro en los que Incident Manager utiliza sus KMS claves. Incident Manager utiliza el siguiente contexto de cifrado:

- `contactArn=ARN of the contact or escalation plan`

Identity and Access Management para AWS Systems Manager Incident Manager

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAM los administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Incident Manager. IAM es un Servicio de AWS que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [¿Cómo AWS Systems Manager Incident Manager funciona con IAM](#)
- [Ejemplos de políticas basadas en identidades de AWS Systems Manager Incident Manager](#)
- [Ejemplos de políticas basadas en recursos para AWS Systems Manager Incident Manager](#)
- [Prevención de suplente confuso entre servicios en Incident Manager](#)
- [Uso de roles vinculados a servicios para Incident Manager](#)
- [AWS políticas gestionadas para AWS Systems Manager Incident Manager](#)
- [Solución de problemas AWS Systems Manager Incident Manager de identidad y acceso](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Incident Manager.

Usuario del servicio: si utiliza el servicio de Incident Manager para realizar su trabajo, su administrador le proporcionará las credenciales y permisos que necesite. A medida que utilice más características de Incident Manager para realizar su trabajo, es posible que necesite permisos

adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica de Incident Manager, consulte [Solución de problemas AWS Systems Manager Incident Manager de identidad y acceso](#).

Administrador del servicio: si está a cargo de los recursos de Incident Manager en su empresa, es probable que tenga acceso completo a Incident Manager. Su trabajo consiste en determinar a qué características y recursos de Incident Manager deben acceder los usuarios de su servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos del IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Incident Manager, consulte [¿Cómo AWS Systems Manager Incident Manager funciona con IAM?](#)

IAM administrador: si es IAM administrador, tal vez le interese obtener más información sobre cómo redactar políticas para administrar el acceso a Incident Manager. Para ver ejemplos de políticas basadas en la identidad de Incident Manager que puede utilizar IAM, consulte [Ejemplos de políticas basadas en identidades de AWS Systems Manager Incident Manager](#)

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol.

Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte [Cómo iniciar sesión Cuenta de AWS en su](#) Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar AWS API las solicitudes](#) en la Guía del IAM usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactorial](#) en la Guía del AWS IAM Identity Center usuario y [Uso de la autenticación multifactorial \(MFA\) AWS en](#) la Guía del IAM usuario.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte [Tareas que requieren credenciales de usuario root](#) en la Guía del IAM usuario.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones Cuentas de AWS . Para obtener información sobre IAM Identity Center, consulte [¿Qué es IAM Identity Center?](#) en la Guía AWS IAM Identity Center del usuario.

Usuarios y grupos de IAM

Un [IAMusuario](#) es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales

temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte [Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración](#) en la Guía del IAM usuario.

Un [IAMgrupo](#) es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte [Cuándo crear un IAM usuario \(en lugar de un rol\)](#) en la Guía del IAM usuario.

IAMroles

Un [IAMrol](#) es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console [cambiando de rol](#). Puede asumir un rol llamando a una AWS API operación AWS CLI o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte [Uso de IAM roles](#) en la Guía del IAM usuario.

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte [Creación de un rol para un proveedor de identidad externo](#) en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.

- **Acceso multicuenta:** puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los [recursos entre cuentas IAM en](#) la Guía del IAM usuario.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
- **Sesiones de acceso directo (FAS):** cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama a un Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FAS las solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros recursos Servicios de AWS o para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar las sesiones de acceso](#).
- **Función de servicio:** una función de servicio es una [IAM función](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte [Crear un rol para delegar permisos Servicio de AWS en un rol](#) en el IAM Manual del usuario.
- **Función vinculada a un servicio:** una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- **Aplicaciones que se ejecutan en Amazon EC2:** puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso dentro de la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales

temporales. Para obtener más información, consulte [Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte [Cuándo crear un IAM rol \(en lugar de un usuario\)](#) en la Guía del IAM usuario.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte [Descripción general de JSON las políticas](#) en la Guía del IAM usuario.

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Las políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte [Creación de IAM políticas](#) en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo

o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte [Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM](#) usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puede usar políticas AWS administradas desde una política IAM basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatibles ACLs. Para obtener más información ACLs, consulte la [descripción general de la lista de control de acceso \(ACL\)](#) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAM usuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo

Principal no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los [límites de los permisos para IAM las entidades](#) en la Guía del IAM usuario.

- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las [políticas de control de servicios](#) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte [las políticas de sesión](#) en la Guía del IAM usuario.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del IAM usuario.

¿Cómo AWS Systems Manager Incident Manager funciona con IAM

Antes de administrar el acceso IAM a Incident Manager, infórmese sobre IAM las funciones disponibles para su uso con Incident Manager.

IAM funciones que puede utilizar con AWS Systems Manager Incident Manager

IAM característica	Soporte de Incident Manager
Políticas basadas en identidades	Sí

IAM característica	Soporte de Incident Manager
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	No
ACLs	No
ABAC(etiquetas en las políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan Incident Manager y otros AWS servicios con la mayoría de IAM las funciones, consulte [AWS los servicios con los que funcionan IAM](#) en la Guía del IAM usuario.

Incident Manager no admite políticas que denieguen el acceso a recursos compartidos mediante AWS RAM.

Políticas basadas en identidades de Incident Manager

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte [Creación de IAM políticas](#) en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones.

No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la [referencia sobre los elementos de la IAM JSON política](#) en la Guía del IAM usuario.

Ejemplos de políticas basadas en identidades de Incident Manager

Para ver ejemplos de políticas basadas en identidades de Incident Manager, consulte [Ejemplos de políticas basadas en identidades de AWS Systems Manager Incident Manager](#).

Políticas basadas en recursos en Incident Manager

Compatibilidad con las políticas basadas en recursos: sí

Las políticas basadas en recursos son documentos JSON de política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Acceso a recursos entre cuentas IAM en](#) la Guía del IAM usuario.

El servicio Incident Manager solo admite dos tipos de políticas basadas en recursos: la AWS RAM consola o la PutResourcePolicy acción, que se adjunta a un plan de respuesta o contacto. Esta política define qué entidades principales pueden realizar acciones en relación con los planes de respuesta, los contactos, los planes de escalada y los incidentes. Incident Manager utiliza políticas basadas en recursos para compartir los recursos entre las cuentas.

Incident Manager no admite políticas que denieguen el acceso a recursos compartidos mediante AWS RAM.

Para obtener información sobre cómo adjuntar una política basada en recursos a un plan de respuesta o a un contacto, consulte [Administración de incidentes entre regiones y entre cuentas en Incident Manager](#).

Ejemplos de políticas basadas en recursos en Incident Manager

Para ver ejemplos de políticas basadas en recursos de Incident Manager, consulte [Ejemplos de políticas basadas en recursos para AWS Systems Manager Incident Manager](#).

Acciones de política de Incident Manager

Compatibilidad con las acciones de política: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de acciones de Incident Manager, consulte [Acciones definidas por AWS Systems Manager Incident Manager](#) en la Referencia de autorización de servicios.

Las acciones de política en Incident Manager utilizan los siguientes prefijos antes de la acción:

```
ssm-incidents  
ssm-contacts
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
```

```
"ssm-incidents:GetResponsePlan",  
"ssm-contacts:GetContact"  
]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra Get, incluya la siguiente acción:

```
"Action": "ssm-incidents:Get*"
```

Para ver ejemplos de políticas basadas en identidades de Incident Manager, consulte [Ejemplos de políticas basadas en identidades de AWS Systems Manager Incident Manager](#).

Incident Manager utiliza acciones en dos espacios de nombre diferentes, ssm-incidents y ssm-contacts. Al crear políticas para Incident Manager, asegúrese de utilizar el espacio de nombres correcto para la acción. SSM-Los incidentes se utilizan para el plan de respuesta y las acciones relacionadas con los incidentes. SSM-Los contactos se utilizan para las acciones relacionadas con los contactos y la interacción con ellos. Por ejemplo:

- ssm-contacts:GetContact
- ssm-incidents:GetResponsePlan

Recursos de políticas para Incident Manager

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento Resource JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento Resource o NotResource. Como práctica recomendada, especifique un recurso mediante su [nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Incident Manager y sus ARNs correspondientes, consulte [los recursos definidos AWS Systems Manager Incident Manager](#) en la Referencia de autorización del servicio. Para saber con qué acciones puede especificar cada recurso, consulte [Acciones definidas por AWS Systems Manager Incident Manager](#). ARN

Para ver ejemplos de políticas basadas en identidades de Incident Manager, consulte [Ejemplos de políticas basadas en identidades de AWS Systems Manager Incident Manager](#).

Los recursos de Incident Manager se utilizan para crear incidentes, colaborar en los canales de chat, resolver incidentes e involucrar al personal de respuesta. Si un usuario tiene acceso a un plan de respuesta, tiene acceso a todos los incidentes creados a partir del mismo. Si un usuario tiene acceso a un contacto o a un plan de escalada puede hacer participar a un contacto (o contactos) en el plan de escalada.

Claves de condiciones de políticas para Incident Manager

Admite claves de condición de política específicas del servicio: No

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación AND lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte [los elementos de IAM política: variables y etiquetas](#) en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del IAMusuario.

Listas de control de acceso (ACLs) en Incident Manager

SoportaACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Control de acceso basado en atributos () ABAC con Incident Manager

Soportes ABAC (etiquetas en las políticas): No

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchos AWS recursos. Etiquetar entidades y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información al respectoABAC, consulte [¿Qué es? ABAC](#) en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte [Usar el control de acceso basado en atributos \(ABAC\)](#) en la Guía del IAMusuario.

Uso de credenciales temporales con Incident Manager

Compatibilidad con credenciales temporales: sí

Algunos Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta la sección [Servicios de AWS Cómo trabajar con credenciales temporales IAM](#) en la Guía del IAM usuario.

Está utilizando credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de rol, consulte [Cambiar a un rol \(consola\)](#) en la Guía del IAM usuario.

Puede crear credenciales temporales manualmente con la tecla AWS CLI o AWS API. A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#).

Permisos de entidades principales entre servicios para Incident Manager

Admite sesiones de acceso directo (FAS): Sí

Cuando utilizas un IAM usuario o un rol para realizar acciones en AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama a un Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. FAS las solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros recursos Servicios de AWS o para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar las sesiones de acceso](#).

Roles de servicio para Incident Manager

Compatibilidad con roles de servicio: sí

Una función de servicio es una [IAM función](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte [Crear un rol para delegar permisos Servicio de AWS en un rol](#) en el IAM Manual del usuario.

⚠ Warning

La modificación de permisos de un rol de servicio puede interrumpir la funcionalidad de Incident Manager. Edite los roles de servicio solo cuando Incident Manager le proporcione orientación para hacerlo.

Elegir un IAM rol en Incident Manager

Al crear un recurso de plan de respuesta en Incident Manager, debe elegir un rol para permitir que Incident Manager ejecute un documento de automatización de Systems Manager en su nombre. Si ha creado previamente un rol de servicio o un rol vinculado al servicio, Incident Manager le proporciona una lista de roles entre los que elegir. Es importante elegir un rol que permita el acceso para ejecutar sus instancias de documentos de automatización. Para obtener más información, consulte [Uso de los manuales de procedimientos de Systems Manager Automation en Incident Manager](#). Al crear un canal de AWS Chatbot chat para usarlo durante un incidente, puede seleccionar un rol de servicio que le permita usar los comandos directamente desde el chat. Para obtener más información sobre la creación de canales de chat para colaboración en incidentes, consulte [Uso de los canales de chat en Incident Manager](#). Para obtener más información sobre IAM las políticas AWS Chatbot, consulte [Administrar los permisos para ejecutar comandos mediante AWS Chatbot](#) la guía AWS Chatbot del administrador.

Roles vinculados a servicios para Incident Manager

Admite roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

Para obtener información sobre la creación o administración de roles vinculados al servicio de Incident Manager, consulte [Uso de roles vinculados a servicios para Incident Manager](#).

Ejemplos de políticas basadas en identidades de AWS Systems Manager Incident Manager

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos de Incident Manager. Tampoco pueden realizar tareas mediante las teclas AWS Management Console,

AWS Command Line Interface (AWS CLI) o. AWS API Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte [Creación de IAM políticas](#) en la Guía del IAM usuario.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Incident Manager, incluido el ARNs formato de cada uno de los tipos de recursos, consulte [las claves de condición, recursos y acciones de la Referencia AWS Systems Manager Incident Manager](#) de autorización de servicio.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la consola de Incident Manager](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)
- [Acceso a un plan de respuesta](#)

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar recursos de Incident Manager en su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Para obtener más información, consulte [las políticas AWS gestionadas](#) o [las políticas AWS gestionadas para las funciones laborales](#) en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos

como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte [Políticas y permisos IAM en](#) la IAM Guía del usuario.

- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse mediante SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte [los elementos IAM JSON de la política: Condición](#) en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAM Access Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la [validación de políticas de IAM Access Analyzer](#) en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte [Configuración del API acceso MFA protegido](#) en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadas IAM, consulte las [prácticas recomendadas de seguridad IAM en](#) la Guía del IAM usuario.

Uso de la consola de Incident Manager

Para acceder a la AWS Systems Manager Incident Manager consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver los detalles de los recursos de Incident Manager en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que están intentando realizar.

Para garantizar que los usuarios y los roles puedan resolver los incidentes mediante la consola de Incident Manager, adjunte también la política `IncidentManagerResolverAccess` AWS gestionada por Incident Manager a las entidades. Para obtener más información, consulte [Añadir permisos a un usuario](#) en la Guía del IAM usuario.

```
IncidentManagerResolverAccess
```

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
    },
  ],
}
```

```

        "Resource": "*"
    }
]
}

```

Acceso a un plan de respuesta

En este ejemplo, quiere conceder a un IAM usuario de su cuenta de Amazon Web Services acceso a uno de sus planes de respuesta de Incident Manager, `exampleplan`. También desea permitir al usuario que añada, actualice y elimine el plan de respuesta.

La política concede los permisos `ssm-incidents:ListResponsePlans`, `ssm-incidents:GetResponsePlan`, `ssm-incidents:UpdateResponsePlan` y `ssm-incident:ListResponsePlan` al usuario.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListResponsePlans",
      "Effect": "Allow",
      "Action": [
        "ssm-incidents:ListResponsePlans"
      ],
      "Resource": "arn:aws:ssm-incidents::*"
    },
    {
      "Sid": "ViewSpecificResponsePlanInfo",
      "Effect": "Allow",
      "Action": [
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource": "arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan"
    },
    {
      "Sid": "ManageResponsePlan",
      "Effect": "Allow",
      "Action": [
        "ssm-incidents:UpdateResponsePlan"
      ],
      "Resource": "arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan/*"
    }
  ]
}

```

```
]
}
```

Ejemplos de políticas basadas en recursos para AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager admite políticas de permisos basadas en recursos para los planes de respuesta y los contactos de Incident Manager.

Incident Manager no admite políticas basadas en recursos que denieguen el acceso a los recursos que se utilizan de forma compartida. AWS RAM

Para obtener información sobre cómo crear un plan de respuesta o un contacto, consulte [Uso de los planes de respuesta en Incident Manager](#) y [Uso de los contactos en Incident Manager](#).

Restricción de acceso al plan de respuesta de Incident Manager por organización

El siguiente ejemplo otorga permisos a los usuarios de la organización con ID de organización o-abc123def45 para que respondan a incidentes creados utilizando el plan de respuesta myplan.

El Condition bloque usa las StringEquals condiciones y la clave de aws:PrincipalOrgID condición, que es una clave de condición AWS Organizations específica. Para obtener más información sobre estas claves de condición, consulte [Especificación de condiciones en una política](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Condition": {
        "StringEquals": {"aws:PrincipalOrgID": "o-abc123def45"}
      },
      "Action": [
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:StartIncident",
        "ssm-incidents:UpdateIncidentRecord",
```

```

    "ssm-incidents:GetIncidentRecord",
    "ssm-incidents:CreateTimelineEvent",
    "ssm-incidents:UpdateTimelineEvent",
    "ssm-incidents:GetTimelineEvent",
    "ssm-incidents:ListTimelineEvents",
    "ssm-incidents:UpdateRelatedItems",
    "ssm-incidents:ListRelatedItems"
  ],
  "Resource": [
    "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
    "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
  ]
}
]
}

```

Concesión de acceso de contactos de Incident Manager a una entidad principal

El siguiente ejemplo concede permiso al director ARN `arn:aws:iam::999988887777:root` para crear interacciones con el contacto. `mycontact`

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PrincipalAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::999988887777:root"
      },
      "Action": [
        "ssm-contacts:GetContact",
        "ssm-contacts:StartEngagement",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:ListPagesByContact"
      ],
      "Resource": [
        "arn:aws:ssm-contacts:*:111122223333:contact/mycontact",
        "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
      ]
    }
  ]
}

```

Prevención de suplente confuso entre servicios en Incident Manager

El problema del suplente confuso es un problema de seguridad que se produce cuando una entidad sin permiso para realizar una acción llama a una entidad con más privilegios para que la realice. Esto puede permitir que actores malintencionados ejecuten comandos o modifiquen recursos para los que, de otro modo, no tendrían permiso de ejecución ni acceso.

En AWS, la suplantación de identidad entre servicios puede llevar a una situación de diputado confusa. La suplantación entre servicios ocurre cuando un servicio (el servicio que realiza las llamadas) llama a otro servicio (el servicio al que se llama). Un actor malintencionado puede utilizar el servicio de llamadas para alterar los recursos de otro servicio mediante permisos que normalmente no tendría.

AWS proporciona a los directores de servicio acceso gestionado a los recursos de tu cuenta para ayudarte a proteger la seguridad de tus recursos. Recomendamos utilizar las claves de contexto de condición global de [aws:SourceArn](#) y [aws:SourceAccount](#) en sus políticas de recursos. Estas claves limitan los permisos que AWS Systems Manager Incident Manager otorgan otro servicio a ese recurso. Si se utilizan ambas claves de contexto de condición global, tanto el valor `aws:SourceAccount` como la cuenta a la que se hace referencia en el valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilicen en la misma instrucción de política.

El valor de `aws:SourceArn` debe ser el ARN del registro de incidentes afectado. Si no conoce la totalidad ARN del recurso o si está especificando varios recursos, utilice la clave de condición del contexto `aws:SourceArn` global con el `*` comodín para las partes desconocidas del ARN. Por ejemplo, puede establecer `aws:SourceArn` para `arn:aws:ssm-incidents::111122223333:*`.

En el siguiente ejemplo de política de confianza, utilizamos la clave de `aws:SourceArn` condición para restringir el acceso a la función de servicio en función del registro del ARN incidente. Solo los registros de incidentes creados a partir del recurso del plan de respuesta `myresponseplan` pueden utilizar este rol.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
```



```
    "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/  
myresponseplan/*"  
  }  
}  
}  
}
```

Uso de roles vinculados a servicios para Incident Manager

AWS Systems Manager Incident Manager usa AWS Identity and Access Management (IAM) roles [vinculados al servicio](#). Un rol vinculado al servicio es un tipo único de IAM rol que está vinculado directamente a Incident Manager. Los roles vinculados al servicio están predefinidos por Incident Manager e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a servicios facilita la configuración de Incident Manager porque no tiene que añadir manualmente los permisos necesarios. Incident Manager define los permisos de sus roles vinculados a servicios y, a menos que se defina de otro modo, solo Incident Manager puede asumir sus roles. Los permisos definidos incluyen la política de confianza y la política de permisos, y esa política de permisos no se puede adjuntar a ninguna otra IAM entidad.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus recursos de Incident Manager porque usted no puede eliminar inadvertidamente el permiso para acceder a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte [AWS Servicios con los que funcionan IAM y busque los servicios con](#) los que se indica Sí en la columna Función vinculada al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios para Incident Manager

Incident Manager utiliza la función vinculada al servicio denominada `AWSServiceRoleforIncidentManager`: permite a Incident Manager gestionar los registros de incidentes de Incident Manager y los recursos relacionados en su nombre.

El rol `AWSServiceRoleforIncidentManager` vinculado al servicio confía en que los siguientes servicios asuman el rol:

- `ssm-incidents.amazonaws.com`

La política de permisos del rol [AWSIncidentManagerServiceRolePolicy](#) permite a Incident Manager realizar las siguientes acciones en los recursos especificados:

- Acción: `ssm-incidents:ListIncidentRecords` en todos los recursos relacionados con la acción.
- Acción: `ssm-incidents:CreateTimelineEvent` en todos los recursos relacionados con la acción.
- Acción: `ssm:CreateOpsItem` en todos los recursos relacionados con la acción.
- Acción: `ssm:AssociateOpsItemRelatedItem` en all resources related to the action.
- Acción: `ssm-contacts:StartEngagement` en todos los recursos relacionados con la acción.
- Acción: `cloudwatch:PutMetricData` en CloudWatch las métricas del espacio de nombres `AWS/IncidentManager`

Debe configurar los permisos para permitir que una IAM entidad (como un usuario, un grupo o un rol) cree, edite o elimine un rol vinculado a un servicio. Para obtener más información, consulte [Permisos de roles vinculados a un servicio](#) en la Guía del usuario. IAM

Creación de un rol vinculado a servicios para Incident Manager

No necesita crear manualmente un rol vinculado a servicios. Al crear un conjunto de réplicas en el AWS Management Console AWS CLI, el administrador de incidentes o el AWS API administrador de incidentes crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un conjunto de réplica, Incident Manager vuelve a crear el rol vinculado a servicios por usted.

Edición de un rol vinculado a servicios para Incident Manager

Incident Manager no le permite editar el rol vinculado al `AWSServiceRoleforIncidentManager` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando. IAM Para obtener más información, consulte [Edición de un rol vinculado a un servicio](#) en la Guía del IAMusuario.

Eliminación de un rol vinculado a servicios para Incident Manager

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitoree ni se mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

Para eliminar el rol vinculado a servicios, primero debe eliminar el conjunto de réplica. Al eliminar el conjunto de réplica se eliminan todos los datos creados y almacenados en Incident Manager, incluyendo los planes de respuesta, contactos y planes de escalada. También pierde todos los incidentes creados anteriormente. Las alarmas y EventBridge reglas que indiquen la eliminación de planes de respuesta dejarán de generar un incidente en caso de alarma o de conformidad con las reglas. Para eliminar el conjunto de réplica debe eliminar todas las regiones del conjunto.

Note

Si el servicio de Incident Manager utiliza el rol al momento de intentar eliminar los recursos, es posible que la eliminación falle. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar las regiones del conjunto de réplicas utilizado por el `AWSServiceRoleforIncidentManager`

1. Abra la [consola de Incident Manager](#) y seleccione Configuración en el panel de navegación izquierdo.
2. Seleccione una región en Conjunto de réplica.
3. Elija Eliminar.
4. Para confirmar la eliminación de la región, introduzca el nombre de la región y elija Eliminar.
5. Repita estos pasos hasta que haya eliminado todas las regiones de su conjunto de réplica. Al eliminar la última región, la consola le notifica que con ella elimina el conjunto de réplica.

Para eliminar manualmente el rol vinculado al servicio mediante IAM

Utilice la IAM consola AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleforIncidentManager` servicio. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) en la Guía del usuario. IAM

Regiones admitidas para los roles vinculados a servicios de Incident Manager

Incident Manager admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte [AWS Puntos de conexión y regiones](#).

AWS políticas gestionadas para AWS Systems Manager Incident Manager

Una política AWS gestionada es una política independiente creada y administrada por AWS. Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir [políticas administradas por el cliente](#) específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando haya nuevas API operaciones disponibles para los servicios existentes.

Para obtener más información, consulte [las políticas AWS administradas](#) en la Guía del IAM usuario.

AWS política gestionada: AWSIncidentManagerIncidentAccessServiceRolePolicy

Puede adjuntarla AWSIncidentManagerIncidentAccessServiceRolePolicy a sus IAM entidades. Incident Manager también asocia esta política a un rol de Incident Manager que permite a Incident Manager realizar acciones en su nombre.

Esta política otorga permisos de solo lectura que permiten a Incident Manager leer los recursos de otros servicios Servicios de AWS para identificar los hallazgos relacionados con los incidentes en esos servicios.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `cloudformation`— Permite a los directores describir las pilas. AWS CloudFormation. Esto es necesario para que el administrador de incidentes identifique CloudFormation los eventos y los recursos relacionados con un incidente.
- `codedeploy`— Permite a los directores leer las AWS CodeDeploy implementaciones. Esto es necesario para que Incident Manager identifique CodeDeploy los despliegues y los objetivos relacionados con un incidente.
- `autoscaling`— Permite a los directores determinar si una instancia de Amazon Elastic Compute Cloud (EC2) forma parte de un grupo de Auto Scaling. Esto es necesario para que Incident Manager pueda proporcionar resultados para EC2 las instancias que forman parte de los grupos de Auto Scaling.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IncidentAccessPermissions",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

Para ver más detalles sobre la política, incluida la versión más reciente del documento de JSON política, consulte [AWSIncidentManagerIncidentAccessServiceRolePolicy](#) la Guía de referencia sobre políticas AWS gestionadas.

Política administrada de AWS : **AWSIncidentManagerServiceRolePolicy**

No puedes asociarte `AWSIncidentManagerServiceRolePolicy` a tus IAM entidades. Esta política se vincula a un rol vinculado a servicios que permite a Incident Manager realizar acciones en su nombre. Para obtener más información, consulte [Uso de roles vinculados a servicios para Incident Manager](#).

Esta política otorga a Incident Manager permisos para enumerar incidentes, crear eventos OpsItems cronológicos, crear OpsItems, asociar elementos relacionados, iniciar interacciones y publicar CloudWatch métricas relacionadas con un incidente.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ssm-incidents`: permite a las entidades principales enumerar incidentes y crear eventos de línea temporal. Resulta necesario para que los respondedores puedan colaborar durante un incidente en el panel de control de incidentes.
- `ssm`— Permite a los directores crear OpsItems y asociar elementos relacionados. Esto es necesario para crear un padre OpsItem cuando se inicia un incidente.
- `ssm-contacts`: permite a las entidades principales iniciar participaciones. Resulta necesario para que Incident Manager involucre a los contactos durante un incidente.
- `cloudwatch`— Permite a los directores publicar CloudWatch métricas. Resulta necesario para que Incident Manager publique las métricas relacionadas con un incidente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateIncidentRecordPermissions",
      "Effect": "Allow",
      "Action": [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    },
    {
      "Sid": "RelatedOpsItemPermissions",
      "Effect": "Allow",
      "Action": [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IncidentEngagementPermissions",
      "Effect": "Allow",
      "Action": "ssm-contacts:StartEngagement",
      "Resource": "*"
    },
    {
      "Sid": "PutCloudWatchMetricPermission",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/IncidentManager"
        }
      }
    }
  ]
}

```

Para ver más detalles sobre la política, incluida la última versión del documento de JSON política, consulte la Guía [AWSIncidentManagerServiceRolePolicy](#) de referencia sobre políticas AWS gestionadas.

AWS política gestionada: **AWSIncidentManagerResolverAccess**

Puede adjuntarla `AWSIncidentManagerResolverAccess` a sus IAM entidades para que puedan iniciar, ver y actualizar incidentes. Esto también les permite crear incidencias en la línea temporal del cliente y elementos relacionados en el panel de control de incidencias. También puedes adjuntar esta política a la función de AWS Chatbot servicio o directamente a la función gestionada por el

cliente asociada a cualquier canal de chat que se utilice para la colaboración en caso de incidentes. Para obtener más información sobre IAM las políticas AWS Chatbot, consulte [Administrar los permisos para ejecutar comandos mediante AWS Chatbot](#) la Guía AWS Chatbot del administrador.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ssm-incidents`: le permite iniciar incidentes, enumerar planes de respuesta, enumerar incidentes, actualizar incidentes, enumerar eventos de línea temporal, crear eventos de línea temporal personalizados, actualizar eventos de línea temporal personalizados, eliminar eventos de línea temporal personalizados, enumerar elementos relacionados, crear elementos relacionados y actualizar elementos relacionados.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "StartIncidentPermissions",
      "Effect": "Allow",
      "Action": [
        "ssm-incidents:StartIncident"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ResponsePlanReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IncidentRecordResolverPermissions",
      "Effect": "Allow",
      "Action": [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:GetIncidentRecord",

```



```

        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents>DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
    ],
    "Resource": "*"
}
]
}

```

Para ver más detalles sobre la política, incluida la versión más reciente del documento de JSON política, consulte [AWSIncidentManagerResolverAccess](#) la Guía de referencia de políticas AWS gestionadas.

Incident Manager actualiza las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas de Incident Manager desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbese al RSS feed de la página del historial de documentos de Incident Manager.

Cambio	Descripción	Fecha
AWSIncidentManagerIncidentAccessServiceRolePolicy — Actualización de la política	Incident Manager ha agregado un nuevo permiso <code>AWSIncidentManagerIncidentAccessServiceRolePolicy</code> , en apoyo de la función Hallazgos, que le permite comprobar si una EC2 instancia forma parte de un grupo de Auto Scaling.	20 de febrero de 2024

Cambio	Descripción	Fecha
AWSIncidentManagerIncidentAccessServiceRolePolicy : política nueva	Incident Manager agregó una nueva política que otorga permisos a Incident Manager para llamar a otros Servicios de AWS personas como parte de la gestión de un incidente.	17 de noviembre de 2023
AWSIncidentManagerServiceRolePolicy — Actualización de la política	Incident Manager agregó un nuevo permiso que le permite a Incident Manager publicar métricas en su cuenta.	16 de diciembre de 2022
AWSIncidentManagerResolverAccess : política nueva	Incident Manager ha añadido una nueva política que permite iniciar incidentes, enumerar planes de respuesta, enumerar incidentes, actualizar incidentes, enumerar eventos de la línea temporal, crear eventos de la línea temporal personalizados, actualizar eventos de la línea temporal personalizados, eliminar eventos de la línea temporal personalizados, enumerar elementos relacionados, crear elementos relacionados y actualizar elementos relacionados.	26 de abril de 2021

Cambio	Descripción	Fecha
AWSIncidentManagerServiceRolePolicy : política nueva	Incident Manager agregó una nueva política que le otorga permisos a Incident Manager para enumerar incidentes, crear eventos cronológicos OpsItems, crear OpsItems, asociar elementos relacionados e iniciar interacciones relacionadas con un incidente.	26 de abril de 2021
Incident Manager comenzó a hacer el seguimiento de cambios	Incident Manager comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	26 de abril de 2021

Solución de problemas AWS Systems Manager Incident Manager de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con Incident Manager y IAM.

Temas

- [No tengo autorización para realizar una acción en Incident Manager](#)
- [No estoy autorizado a realizar tareas como: PassRole](#)
- [Deseo permitir que personas ajenas a mi cuenta de Amazon Web Services puedan acceder a mis recursos de Incident Manager](#)

No tengo autorización para realizar una acción en Incident Manager

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para ver los detalles de un `my-example-widget` recurso ficticio, pero no tiene los `ssm-incidents:GetWidget` permisos ficticios.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: ssm-incidents:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso `my-example-widget` mediante la acción `ssm-incidents:GetWidget`.

Si necesita ayuda, póngase en contacto con AWS el administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Incident Manager.

Algunos Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario denominado `marymajor` intenta utilizar la consola para realizar una acción en Incident Manager. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Deseo permitir que personas ajenas a mi cuenta de Amazon Web Services puedan acceder a mis recursos de Incident Manager

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para

que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede utilizar esas políticas para permitir que las personas accedan a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Incident Manager admite estas características, consulte [¿Cómo AWS Systems Manager Incident Manager funciona con IAM.](#)
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta [Cómo proporcionar acceso a un IAM usuario en otro de tu Cuenta de AWS propiedad](#) en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta [Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(federación de identidades\)](#) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a [recursos entre cuentas IAM en la Guía](#) del usuario. IAM

Uso compartido de contactos y planes de respuesta en Incident Manager

Con el uso compartido de contactos, como propietario de un contacto, puede compartir la información de contacto, los planes de escalamiento y las interacciones con otras Cuentas de AWS personas o dentro de una organización. AWS Puede crear y administrar contactos y planes de escalada de forma centralizada y asegurarse de que los demás puedan involucrar a los contactos correctos durante un incidente.

Al compartir un plan de respuesta, como propietario del plan de respuesta, puede compartir un plan de respuesta y los incidentes relacionados con otros Cuentas de AWS o dentro de una AWS organización. Puede crear y administrar planes de respuesta de forma centralizada para que los respondedores de las cuentas de consumidores puedan interactuar con los incidentes a medida que se producen.

El propietario de un contacto o de un plan de respuesta puede compartir contactos y planes de respuesta con:

- Cuentas de AWS Específico dentro o fuera de su organización en AWS Organizations
- Una unidad organizativa dentro de su organización en AWS Organizations
- Toda su organización en AWS Organizations

Contenido

- [Requisitos previos para compartir contactos y planes de respuesta](#)
- [Servicios relacionados](#)
- [Uso compartido de un contacto o un plan de respuesta](#)
- [Detención del uso compartido de un contacto o un plan de respuesta](#)
- [Identificación de un contacto o plan de respuesta compartidos](#)
- [Permisos de los contactos y planes de respuesta compartidos](#)
- [Facturación y medición](#)
- [Límites de instancias](#)

Requisitos previos para compartir contactos y planes de respuesta

Para compartir un contacto o un plan de respuesta con su organización o unidad organizativa en AWS Organizations:

- Debe ser propietario del recurso en su Cuenta de AWS. No puede compartir un contacto o plan de respuesta que se haya compartido con usted.
- Debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte [Habilitar el uso compartido con AWS Organizations](#) en la Guía del usuario de AWS RAM .

Servicios relacionados

El uso compartido de contactos y planes de respuesta se integra con AWS Resource Access Manager (AWS RAM). Con AWS RAM, puede compartir sus AWS recursos con cualquiera Cuenta de AWS o mediante AWS Organizations. Puede compartir los recursos que posea creando un Uso compartido de recursos. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los consumidores pueden ser individuos Cuentas de AWS, unidades organizativas o toda una organización AWS Organizations.

Para obtener más información al respecto AWS RAM, consulte la [Guía AWS RAM del usuario](#).

Uso compartido de un contacto o un plan de respuesta

Después de compartir un plan de respuesta, los consumidores tienen acceso a todos los incidentes pasados, actuales y futuros creados con el uso de ese plan de respuesta.

Después de compartir un contacto, los consumidores tienen acceso a la información de contacto, el plan de participación, los planes de escalada y las participaciones que tengan lugar durante un incidente. Los consumidores también pueden acceder a un contacto o a un plan de escalada durante un incidente.

Si forma parte de una organización AWS Organizations y está activado el uso compartido dentro de su organización, los consumidores de su organización tienen acceso automático al contacto compartido o al plan de respuesta. Caso contrario, los consumidores reciben una invitación para unirse al uso compartido del recurso y se les concede acceso al contacto o plan de respuesta compartido tras aceptar la invitación.

Puedes compartir un contacto o un plan de respuesta de tu propiedad mediante la AWS RAM consola o el AWS CLI.

Para compartir un contacto o un plan de respuesta de tu propiedad mediante la AWS RAM consola

Consulte [Crear un recurso compartido](#) en la Guía del usuario de AWS RAM .

Para compartir un contacto o un plan de respuesta de tu propiedad mediante el AWS CLI

Usa el [create-resource-share](#) comando.

Detención del uso compartido de un contacto o un plan de respuesta

Cuando el propietario de un recurso deja de compartir un contacto o un plan de respuesta con un consumidor, los contactos, planes de respuesta, planes de escalada, participaciones e incidentes dejan de aparecer en la consola del consumidor.

Note

El consumidor seguirá viendo los contactos, planes de respuesta, planes de escalada, participaciones e incidentes sin actualizaciones, si los ve en la consola, hasta que actualice la página o salga de ella.

Para dejar de compartir un contacto o plan de respuesta compartido de su propiedad, debe eliminarlo del recurso compartido. Puede hacerlo mediante la AWS RAM consola o el AWS CLI.

Para dejar de compartir un contacto o plan de respuesta compartido de su propiedad mediante la consola de AWS RAM

Consulte [Actualizar un recurso compartido](#) en la Guía del usuario de AWS RAM .

Para dejar de compartir un contacto o plan de respuesta compartido de su propiedad mediante la AWS CLI

Utilice el [disassociate-resource-share](#) comando.

Identificación de un contacto o plan de respuesta compartidos

Los propietarios y los consumidores pueden identificar los contactos y planes de respuesta compartidos mediante la consola de Incident Manager y la AWS CLI.

Para identificar un contacto o plan de respuesta compartidos mediante la consola de Incident Manager

Note

Los contactos, planes de respuesta, planes de escalada, participaciones e incidentes no suelen ser identificables como recursos compartidos en la consola de Incident Manager. En los lugares donde está visible el nombre del recurso de Amazon (ARN), ARN contiene el ID de cuenta del propietario.

Para identificar un contacto compartido o un plan de respuesta mediante el AWS CLI

Utilice los [ListContacts](#) comandos [ListResponsePlans](#). El comando devuelve los contactos y planes de respuesta que le pertenecen y aquellos que se comparten con usted. ARN Muestra el Cuenta de AWS ID del propietario del contacto o del plan de respuesta.

Permisos de los contactos y planes de respuesta compartidos

Permisos de los propietarios

Los propietarios pueden actualizar, ver, compartir, dejar de compartir y utilizar los contactos y planes de respuesta. Los contactos y planes de respuesta incluyen las participaciones y los incidentes relacionados.

Permisos de los consumidores

Los consumidores pueden utilizar y ver solo los planes de respuesta y los contactos. Los contactos y planes de respuesta incluyen las participaciones y los incidentes relacionados.

Facturación y medición

Al propietario del recurso se le factura por el recurso. No se factura a los consumidores por los recursos compartidos con ellos. Compartir un recurso no conlleva costos adicionales.

Límites de instancias

Compartir un recurso no afecta a los límites del recurso en la cuenta del propietario o del consumidor. Solo se utiliza la cuenta del propietario para calcular los límites del recurso.

Validación de conformidad para AWS Systems Manager Incident Manager


Los auditores externos evalúan la seguridad y el cumplimiento AWS Systems Manager Incident Manager como parte de varios programas de AWS cumplimiento. Estos incluyen SOC PCI la Reserva Federal RAMP HIPAA y otros.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa](#) de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- [Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

 Note

No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la [Referencia de servicios HIPAA aptos](#).

- [AWS Recursos](#) de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Este Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos

de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.

- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Systems Manager Incident Manager

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

[Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS](#)

Incident Manager es un servicio global-regional y actualmente no admite zonas de disponibilidad.

Además de la infraestructura AWS global, Incident Manager ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos. Durante el asistente de preparación se le pedirá que configure un conjunto de réplica. Este conjunto de réplica regional garantiza que sus datos y recursos sean accesibles desde varias regiones, lo cual hace que la administración de incidentes a través de una red en la nube sea más fácil de administrar. Esta réplica también garantiza que sus datos estén seguros y sean accesibles en caso de que una de sus regiones cayese.

Para obtener más información sobre el uso del conjunto de réplica de Incident Manager, consulte [Uso del conjunto de réplica de Incident Manager](#).

Seguridad de la infraestructura en AWS Systems Manager Incident Manager

Como servicio gestionado, AWS Systems Manager Incident Manager está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo

se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

APIs llamadas AWS publicadas se utilizan para acceder a Incident Manager a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta que esté asociada a un director. IAM También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Trabajar con VPC puntos finales AWS Systems Manager Incident Manager e interconectarse ()AWS PrivateLink

Puede establecer una conexión privada entre su interfaz VPC y la suya AWS Systems Manager Incident Manager mediante la creación de un VCPunto final de interfaz. Puntos de enlace de tipo interfaz con tecnología de AWS PrivateLink. Con él AWS PrivateLink, puede acceder de forma privada a API las operaciones de Incident Manager sin una pasarela de Internet, NAT dispositivo, VPN conexión o AWS Direct Connect conexión. Las instancias VPC que tenga no necesitan direcciones IP públicas para comunicarse con las API operaciones de Incident Manager. El tráfico entre usted VPC y Incident Manager permanece dentro de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más [interfaces de red elásticas](#) en las subredes.

Para obtener más información, consulte [Interface VPC endpoints \(AWS PrivateLink\)](#) en la Guía del VPC usuario de Amazon.

Consideraciones sobre los puntos finales de Incident Manager VPC

Antes de configurar un VPC punto final de interfaz para Incident Manager, asegúrese de revisar las [propiedades, limitaciones y AWS PrivateLink cuotas del punto final de interfaz](#) en la Guía del VPC usuario de Amazon.

Incident Manager permite realizar llamadas a todas sus API acciones desde su cuenta VPC. Para utilizar todo Incident Manager, debe crear dos VPC puntos de conexión: uno para `ssm-incidents` y otro para `ssm-contacts`.

Crear un VPC punto final de interfaz para Incident Manager

Puede crear un VPC punto final para Incident Manager mediante la VPC consola de Amazon o con AWS Command Line Interface (AWS CLI). Para obtener más información, consulte [Creación de un punto final de interfaz](#) en la Guía del VPC usuario de Amazon.

Cree un VPC punto final para Incident Manager con los siguientes nombres de servicio:

- `com.amazonaws.region.ssm-incidents`
- `com.amazonaws.region.ssm-contacts`

Si usa privado DNS para el punto final, puede realizar API solicitudes a Incident Manager utilizando su DNS nombre predeterminado para la región. Por ejemplo, puede utilizar los nombres `ssm-incidents.us-east-1.amazonaws.com` o `ssm-contacts.us-east-1.amazonaws.com`.

Para obtener más información, consulte [Acceder a un servicio a través de un punto final de interfaz](#) en la Guía del VPC usuario de Amazon.

Creación de una política VPC de puntos finales para Incident Manager

Puede adjuntar una política de puntos finales a su VPC punto final que controle el acceso a Incident Manager. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos sobre los que se pueden realizar estas acciones.

Para obtener más información, consulta [Cómo controlar el acceso a los servicios con VPC puntos de conexión](#) en la Guía del VPC usuario de Amazon.

Ejemplo: política de VPC puntos finales para las acciones de Incident Manager

A continuación, se muestra un ejemplo de una política de punto de conexión para Incident Manager. Cuando se vincula a un punto de conexión, esta política otorga acceso a las acciones de Incident Manager enumeradas para todas las entidades principales en todos los recursos.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "ssm-contacts:ListContacts",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:StartIncident"
      ],
      "Resource": "*"
    }
  ]
}
```

Configuración y análisis de vulnerabilidades en Incident Manager

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el [modelo de responsabilidad AWS compartida](#).

Mejores prácticas de seguridad en AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager proporciona muchas características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Temas

- [Prácticas recomendadas de seguridad preventivas para Incident Manager](#)
- [Las mejores prácticas recomendadas de seguridad de detección para Incident Manager](#)

Prácticas recomendadas de seguridad preventivas para Incident Manager

Implementación del acceso a los privilegios mínimos

Al conceder permisos, usted decide quién obtiene determinados permisos en determinados recursos de Incident Manager. Habilite las acciones específicas que desea permitir en dichos recursos. Por lo tanto, conceda solo los permisos necesarios para realizar una tarea. La implementación del acceso con privilegios mínimos es esencial a la hora de reducir los riesgos de seguridad y el impacto que podrían causar los errores o los intentos malintencionados.

Las siguientes herramientas están disponibles para implementar el acceso a los privilegios mínimos:

- [Controlar el acceso a AWS los recursos mediante políticas y límites de permisos para IAM las entidades](#)
- [Políticas de control de servicios](#)

Creación y administración de contactos

Al activar contactos, Incident Manager se pone en contacto con el dispositivo para confirmar la activación. Asegúrese de que la información del dispositivo sea correcta antes de activarlo. Esto reduce la posibilidad de que Incident Manager se ponga en contacto con un dispositivo o persona equivocados durante la activación.

Revise regularmente sus contactos y planes de escalada para asegurarse de que solo se contacte a contactos que deban ser contactados durante un incidente. Revise periódicamente los contactos a fin de eliminar información obsoleta o incorrecta. Si un contacto ya no debe ser informado al producirse un incidente, elimínelo de los planes de escalada relacionados o de Incident Manager.

Privacidad de los canales de chat

Puede hacer que sus canales de chat de incidentes sean privados para implementar el acceso de privilegio mínimo. Considere la posibilidad de utilizar un canal de chat diferente con una lista de usuarios reducida para cada plantilla del plan de respuesta. Esto garantiza que solo los respondedores correctos entren en un canal de chat que pueda contener información sensible.

AWS Chatbot los canales de Slack habilitados heredan los permisos del IAM rol utilizado para configurarlos. AWS Chatbot Esto permite al personal de respuesta de un canal de Slack AWS Chatbot habilitado solicitar cualquier acción de la lista de permitidos, como el administrador de incidentes o la recuperación de gráficos de métricas. APIs

Mantén las herramientas actualizadas AWS

AWS publica periódicamente versiones actualizadas de herramientas y complementos que puede utilizar en sus AWS operaciones. Mantener estos recursos actualizados garantiza que los usuarios y

las instancias de su cuenta tengan acceso a la funcionalidad y las características de seguridad más recientes de estas herramientas.

- **AWS CLI** — The AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te permite interactuar con AWS los servicios mediante comandos de tu consola de línea de comandos. Para actualizar la AWS CLI, ejecute el mismo comando utilizado para instalar la AWS CLI. Recomendamos crear una tarea programada en el equipo local que ejecute el comando apropiado para su sistema operativo al menos una vez cada dos semanas. Para obtener información sobre los comandos de instalación, consulte [Instalación de la interfaz de línea de AWS comandos](#) en la Guía del usuario de la interfaz de línea de AWS comandos.
- **AWS Tools for Windows PowerShell** — Las herramientas para Windows PowerShell son un conjunto de PowerShell módulos que se basan en las funciones expuestas en el AWS SDK formulario. NET. Las herramientas para Windows le PowerShell permiten programar las operaciones de sus AWS recursos desde la línea de PowerShell comandos. Periódicamente, a medida que PowerShell se publiquen versiones actualizadas de las Herramientas para Windows, debe actualizar la versión que esté ejecutando localmente. Para obtener más información, consulte [Actualización de AWS Tools for Windows PowerShell en Windows](#) o [Actualización de AWS Tools for Windows PowerShell en Linux o macOS](#).

Contenido relacionado

[Mejores prácticas de seguridad para Systems Manager](#)

Las mejores prácticas recomendadas de seguridad de detección para Incident Manager

Identificación y auditoría de todos sus recursos de Incident Manager

La identificación de sus activos de TI es un aspecto fundamental de seguridad y control. Identifique sus recursos de Systems Manager para evaluar su postura de seguridad y tomar medidas en las posibles áreas de debilidad. Cree grupos de recursos para sus recursos de Incident Manager. Para obtener más información, consulte [¿Qué son los grupos de recursos?](#) en la Guía del usuario de AWS Resource Groups .

Utilice AWS CloudTrail

AWS CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Incident Manager. Con la información recopilada AWS CloudTrail, puede determinar la

solicitud que se realizó a Incident Manager, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales. Para obtener más información, consulte [Registro de llamadas a la AWS Systems Manager Incident Manager API mediante AWS CloudTrail](#).

Supervise los avisos AWS de seguridad

Compruebe periódicamente los avisos de seguridad publicados en Trusted Advisor su nombre. Cuenta de AWS Puede hacerlo mediante programación usando. [describe-trusted-advisor-checks](#)

Además, supervise activamente la dirección de correo electrónico principal registrada para cada uno de sus. Cuentas de AWS AWS se pondrá en contacto con usted, utilizando esta dirección de correo electrónico, para informarle sobre los problemas de seguridad emergentes que puedan afectarle.

AWS los problemas operativos con un amplio impacto se publican en el [AWS Service Health Dashboard](#). Los problemas operativos también se publican en las cuentas individuales a través de AWS Health Dashboard. Para obtener más información, consulte la [Documentación de AWS Health](#).

Contenido relacionado

[Amazon Web Services: información general de procesos de seguridad](#) (documento técnico)

[Cómo empezar: siga las prácticas recomendadas de seguridad al configurar sus AWS recursos](#) (blog AWS de seguridad)

[IAMPrácticas recomendadas](#)

[Mejores prácticas de seguridad en AWS CloudTrail](#)

Supervisión en Incident Manager

AWS Systems Manager Incident Manager se integra con los siguientes servicios que ofrecen capacidades de monitoreo y registro:

CloudWatch métricas

Utilice CloudWatch las métricas para recuperar estadísticas sobre los puntos de datos de las operaciones de AWS Systems Manager Incident Manager como un conjunto ordenado de datos de series temporales, conocidos como métricas. Utilice estas métricas para comprobar que el sistema funciona de acuerdo con lo esperado. Para obtener más información, consulte [CloudWatch Métricas de Amazon en Incident Manager](#).

CloudTrail registros

Se utiliza AWS CloudTrail para capturar información detallada sobre las llamadas realizadas a AWS las API. Puede almacenar estas llamadas como archivos de registro en Amazon Simple Storage Service. Puede usar estos CloudTrail registros para determinar información como qué llamada se realizó, la dirección IP de origen de la llamada, quién hizo la llamada y cuándo se realizó la llamada. Los CloudTrail registros contienen información sobre las llamadas a las acciones de la API de Incident Manager. IPara obtener más información, consulte [Registro de llamadas a la AWS Systems Manager Incident Manager API mediante AWS CloudTrail](#).

Trusted Advisor

AWS Trusted Advisor puede ayudarlo a monitorear sus AWS recursos para mejorar el rendimiento, la confiabilidad, la seguridad y la rentabilidad. Hay cuatro Trusted Advisor comprobaciones disponibles para todos los usuarios; hay más de 50 comprobaciones disponibles para los usuarios con un plan de soporte empresarial o empresarial. En el caso de Incident Manager, Trusted Advisor comprueba que la configuración de un conjunto de replicación utilice más de una Región de AWS para admitir la conmutación por error y la respuesta regionales. Para obtener más información, consulte [AWS Trusted Advisor](#) en la Guía del usuario de AWS Support .

CloudWatch Métricas de Amazon en Incident Manager

Incident Manager proporciona métricas agregadas que puedes monitorear en Amazon CloudWatch. Puede utilizar estas métricas para identificar las tendencias de los incidentes y los planes de respuesta.

Estas métricas incluyen:


- Número de incidentes creados en un determinado periodo.
- Tiempo de respuesta y resolución de esos incidentes
- Número de incidentes resueltos

Puede monitorear las métricas de Incident Manager para comprender mejor su estado operativo y tomar medidas significativas para impulsar la excelencia operativa de su respuesta a incidentes. Las métricas de Incident Manager están disponibles en todas las regiones de Incident Manager. Sus métricas estarán disponibles para consultarlas en Amazon CloudWatch en todas las regiones que especificó en su conjunto de replicaciones al incorporarse a Incident Manager. Puede ver las métricas publicadas en la región en la que se realizaron acciones para el incidente. No hay ningún cargo adicional por estas métricas.

En la CloudWatch consola, puede crear paneles con estas métricas para:

- Medir y revisar su carga de incidentes existente
- Realizar un seguimiento de si su carga de incidentes aumenta, disminuye o permanece igual
- Utilizar con mayor eficacia Incident Manager para reducir la frecuencia, la duración y el impacto de sus incidentes.

En esta página, se describen las métricas de Incident Manager disponibles en la CloudWatch consola.

 Important

En el caso de un evento generado por un cliente, si el nombre del valor de [origen](#) en `TriggerDetails` se utiliza caracteres que no son ASCII, las métricas del evento no se incluirán en las CloudWatch métricas de Amazon, que no admite texto que no sea ASCII. `sources` solo se puede proporcionar mediante programación, por ejemplo, mediante un SDK o el AWS CLI

Incident Manager envía las siguientes métricas a CloudWatch.

Métrica	Descripción
<code>NumberOfCreateIncidents</code>	<p>Número de incidentes creados.</p> <p>Dimensiones válidas: [] (dimensión vacía), [ResponsePlan], [Impact], [Source], [ResponsePlan , Impact], [ResponsePlan , Source]</p> <p>Unidad: recuento</p>
<code>NumberOfResolveIncidents</code>	<p>Número de incidentes resueltos.</p> <p>Dimensiones válidas: [] (dimensión vacía), [ResponsePlan], [Impact], [Source], [ResponsePlan , Impact], [ResponsePlan , Source]</p> <p>Unidad: recuento</p>
<code>TimeToFirstAcknowledgement</code>	<p>Diferencia de tiempo entre la hora de creación del incidente y la hora en que se realizó el primer acuse de recibo del mismo.</p> <p>Dimensiones válidas: [] (dimensión vacía), [ResponsePlan], [Impact], [Source], [ResponsePlan , Impact], [ResponsePlan , Source]</p> <p>Unidad: segundos</p>
<code>TimeToResolveIncident</code>	<p>Diferencia de tiempo entre el momento en que se creó el incidente y el momento en que se resolvió.</p> <p>Dimensiones válidas: [] (dimensión vacía), [ResponsePlan], [Impact], [Source], [ResponsePlan , Impact], [ResponsePlan , Source]</p>

Métrica	Descripción
	Unidad: segundos

Visualización de las métricas de Incident Manager en la CloudWatch consola

Para ver las métricas de Incident Manager en la CloudWatch consola

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de IncidentManager.
4. En la pestaña Métricas, elija una dimensión y, a continuación, elija una métrica.

Para obtener más información sobre cómo trabajar con CloudWatch métricas, consulta los siguientes temas de la Guía del CloudWatch usuario de Amazon:

- [Métricas](#)
- [Uso de CloudWatch las métricas de Amazon](#)

Dimensiones de métricas

Las métricas de Incident Manager utilizan el espacio de nombres IncidentManager y proporciona métricas para las siguientes dimensiones:

Dimensión	Descripción
By Response Plan	Visualiza las métricas agregadas por plan de respuesta.
By Impact Level	Visualiza las métricas agregadas por el nivel de gravedad.

Dimensión	Descripción
By Source	Consulta las métricas de los incidentes creados manualmente, por CloudWatch alarma o EventBridge evento.
Across All Incidents	Visualiza las métricas agregadas para todos los incidentes en la región de AWS actual.
Response Plan name and Source	Visualiza las métricas agregadas para cada combinación de plan de respuesta y origen.
Response Plan Name and Impact Level	Visualiza las métricas agregadas para cada combinación de plan de respuesta y nivel de gravedad.

Registro de llamadas a la AWS Systems Manager Incident Manager API mediante AWS CloudTrail

AWS Systems Manager Incident Manager está integrado con [AWS CloudTrail](#) un servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un Servicio de AWS. CloudTrail captura todas las llamadas a la API de Incident Manager como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Incident Manager y las llamadas de código a las operaciones de la API de Incident Manager. Con la información recopilada CloudTrail, puede determinar la solicitud que se realizó a Incident Manager, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en tu cuenta Cuenta de AWS cuando creas la cuenta y tienes acceso automáticamente al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWS Para obtener más información, consulte Cómo [trabajar con el historial de CloudTrail eventos en la Guía del usuario](#). AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o [CloudTrail lagos](#).

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte [Creación de un registro de seguimiento para su Cuenta de AWS](#) y [Creación de un registro de seguimiento para una organización](#) en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte [AWS CloudTrail Precios](#). Para obtener información acerca de los precios de Amazon S3, consulte [Precios de Amazon S3](#).

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato [Apache](#) ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando [selectores de eventos avanzados](#). Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo [trabajar con AWS CloudTrail Lake](#) en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, elige la [opción de precios](#) que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte [AWS CloudTrail Precios](#).

Eventos de gestión de incidentes de Incident Manager en CloudTrail

[Los eventos de administración](#) proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

AWS Systems Manager Incident Manager registra todas las operaciones del plano de control de Incident Manager como eventos de gestión. Para obtener una lista de las operaciones del plano de AWS Systems Manager Incident Manager control en las que Incident Manager registra CloudTrail, consulte la [referencia de la AWS Systems Manager Incident Manager API](#).

Ejemplos de eventos de Incident Manager

Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación de API solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que los eventos no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la StartIncident acción.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "1234567890abcdef0",
    "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
    "accountId": "abcdef01234567890",
    "accessKeyId": "021345abcdef6789",
    "userName": "nikki_wolf"
  },
}
```



```

    "eventTime": "2024-04-22T23:20:10Z",
    "eventSource": "ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/ssmincidents.start-incident",
    "requestParameters": {
      "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-test-response-plan-non-dedupe-v1",
      "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
    "responseElements": {
      "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567890",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
  }
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `DeleteContactChannel` acción.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "1234567890abcdef0",
    "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
    "accountId": "abcdef01234567890",
    "accessKeyId": "021345abcdef6789",
    "userName": "nikki_wolf"
  },
  "eventTime": "2024-04-08T02:27:21Z",
  "eventSource": "ssm-contacts.amazonaws.com",
  "eventName": "DeleteContactChannel",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.0",

```

```
"userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
"requestParameters": {
  "contactChannelId": "arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
},
"responseElements": null,
"requestID": "abcdefgh-1234-abcd-1234-1234567890",
"eventID": "12345678-1234-1234-abcd-1234567890",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "12345678901234567"
}
```

Para obtener información sobre el contenido de los CloudTrail registros, consulte el [contenido de los CloudTrail registros](#) en la Guía del AWS CloudTrail usuario.

Integraciones de productos y servicios con Incident Manager

El administrador de incidentes, una capacidad de AWS Systems Manager, se integra con los siguientes productos, servicios y herramientas.

Integración con Servicios de AWS

Incident Manager se integra con Servicios de AWS las herramientas que se describen en la siguiente tabla.

AWS CDK

AWS CDK Se trata de un marco de desarrollo o que permite utilizar código para definir la infraestructura de la nube y utilizarlo AWS CloudFormation para el aprovisionamiento. AWS CDK Es compatible con varios lenguajes de programación TypeScript, incluidos, JavaScript PythonJava, y C#/.Net.

Para obtener información sobre el uso de AWS CDK Incident Manager, consulte las siguientes secciones de la referencia de la AWS CDK API:

- [Módulo de @aws-cdk/aws-ssmincidents](#)
- [Módulo de @aws-cdk/aws-ssmcontacts](#)

AWS Chatbot

AWS Chatbot permite DevOps a los equipos de desarrollo de software utilizar las salas de chat de los programas de mensajería para monitorear y responder a los eventos operativos en sus Nube de AWS

Al utilizar AWS Chatbot Incident Manager, puede crear canales de chat que los socorristas puedan utilizar para supervisar los incidentes y responder a ellos. AWS Chatbot admite salas de Slack chat, Microsoft Teams canales y

salas de chat de Amazon Chime como canales de chat.

Como parte de la creación de un canal de chat, también crea un tema en Amazon Simple Notification Service (Amazon SNS). [Amazon SNS](#) es un servicio administrado que realiza la entrega de mensajes de los publicadores a los suscriptores. En los planes de respuesta a incidentes, al asociar un canal de chat que haya creado con el plan, también elige uno o varios temas que haya asociado al canal de chat. Estos temas de SNS se utilizan para enviar notificaciones sobre un incidente a los respondedores del mismo.

Para obtener más información, consulte [Uso de los canales de chat en Incident Manager](#).

AWS CloudFormation

AWS CloudFormation es un servicio que puede usar para crear una plantilla con todos los recursos que necesita para su aplicación y, a continuación, configurar y aprovisionar los recursos por usted. También configurará todas las dependencias, para que pueda centrarse más en su aplicación y menos en administrar los recursos.

Para obtener información sobre su uso AWS CloudFormation con Incident Manager, consulte los siguientes temas de la [Guía del AWS CloudFormation usuario](#):

- [Referencia de tipo de recurso de Incident Manager](#)
- [Referencia de tipo de recurso de Contactos](#)

Amazon CloudWatch

[CloudWatch](#) supervisa sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir para sus recursos y aplicaciones.

Puede configurar CloudWatch las alarmas para crear incidentes en Incident Manager. CloudWatch trabaja con Systems Manager e Incident Manager para crear un incidente a partir de una plantilla de plan de respuesta cuando una alarma pasa al estado de alarma.

Para obtener más información, consulte [Creación automática de incidentes con alarmas de CloudWatch](#).

Amazon Chime

[Amazon Chime](#) es un lugar de trabajo en línea que combina reuniones, chat y llamadas de negocios. Con Amazon Chime puede reunirse, chatear y realizar llamadas de negocios dentro y fuera de su organización.

Puede integrar una sala de Amazon Chime en sus operaciones de Incident Manager mediante la creación de un canal de chat para Amazon Chime en [AWS Chatbot](#) y la adición a continuación de dicho canal en un plan de respuesta.

Para obtener más información, consulte [Uso de los canales de chat en Incident Manager](#).

Amazon EventBridge

[EventBridge](#) es un servicio sin servidor que utiliza eventos para conectar los componentes de la aplicación, lo que facilita la creación de aplicaciones escalables basadas en eventos.

Puede configurar EventBridge reglas para detectar los patrones de eventos en sus AWS recursos y crear un incidente en Incident Manager cuando un evento coincida con un patrón que haya definido. Sus reglas pueden monitorear los patrones de eventos en docenas de aplicaciones Servicios de AWS y servicios de terceros y de terceros.

Para obtener más información, consulte [Creación automática de incidentes con eventos de EventBridge](#).

AWS Secrets Manager

El [Administrador de secretos](#) le ayuda a administrar, recuperar y rotar credenciales de bases de datos, credenciales de aplicaciones, tokens OAuth, claves API y otros secretos a lo largo de sus ciclos de vida.

Al integrar Incident Manager con el PagerDuty servicio, crea un secreto en Secrets Manager que contiene sus PagerDuty credenciales.

Para obtener más información, consulte [Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager](#).

AWS Systems Manager

[Systems Manager](#) es un centro de operaciones que puede usar para ver y controlar la infraestructura de aplicaciones y una solución de end-to-end administración segura para entornos de nube. Las siguientes funciones de Systems Manager se integran directamente con Incident Manager:

- [Automatización](#): un manual de procedimientos de automatización define las acciones que Systems Manager realiza en sus recursos de AWS. En Incident Manager, un manual de procedimientos define una serie de pasos automatizados y manuales para resolver sus incidentes.

Para obtener información sobre la creación de manuales de procedimientos de automatización para su uso con Incident Manager, consulte [Uso de los manuales de procedimientos de Systems Manager Automation en Incident Manager](#).

- [OpsCenter](#)— OpsCenter proporciona una ubicación central donde los ingenieros de operaciones y los profesionales de TI pueden gestionar los elementos de trabajo operativos OpsItems, denominados «relacionados con AWS los recursos». Puede crear OpsItems directamente a partir de un análisis posterior al incidente para realizar un seguimiento del trabajo relacionado.

Para obtener más información, consulte [Realización de un análisis post-incidente en Incident Manager](#).

AWS Trusted Advisor

[Trusted Advisor](#) es una herramienta disponible para AWS los clientes con un plan de soporte básico o para desarrolladores. Trusted Advisor inspecciona su AWS entorno y, a continuación, hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad.

En el caso de Incident Manager, Trusted Advisor comprueba que la configuración de un conjunto de replicación utilice más de uno Región de AWS para admitir la conmutación por error y la respuesta regionales.

Integración a otros productos y servicios

Puede integrar o utilizar Incident Manager con los servicios de terceros que se describen en la siguiente tabla.

Jira Cloud

Con él AWS Service Management Connector , puedes integrar Incident Manager con [Jira Cloud](#) (Atlassian), una plataforma de flujo de trabajo de terceros basada en la nube.

Después de configurar la integración con Jira Cloud, al crear un nuevo incidente en Incident Manager, la integración crea también el incidente en Jira Cloud. Si actualiza un incidente en Incident Manager, realiza estas actualizaciones en el incidente correspondiente en Jira Cloud. Si resuelve un incidente en Incident Manager o en Jira Cloud, la integración resuelve el incidente en ambos servicios en función de las preferencias que configure.

Para obtener más información, consulta [Integración AWS Systems Manager Incident Manager \(Jira Cloud\)](#) en la Guía del administrador. AWS Service Management Connector

Administración de servicios de Jira

Con ella AWS Service Management Connector , puedes integrar Incident Manager con [Jira Service Management](#), una plataforma de flujo de trabajo de terceros basada en la nube.

Después de configurar la integración con el Administrador de servicios de Jira, al crear un nuevo incidente en Incident Manager, la integración crea también el incidente en el Administrador de servicios de Jira. Si actualiza un incidente en Incident Manager, realiza estas actualizaciones en el incidente correspondiente en el Administrador de servicios de Jira. Si resuelve un incidente en Incident Manager o en el Administrador de servicios de Jira, la integración resuelve el incidente en ambos servicios en función de las preferencias que configure.

Para obtener más información, consulte [Configuración del administrador de servicios de Jira](#) en la Guía del administrador de AWS Service Management Connector .

Microsoft Teams

[Microsoft Teams](#) proporciona herramientas de colaboración basadas en la nube para mensajería en equipo, audioconferencias y videoconferencias, y uso compartido de archivos.

Puede integrar un canal de Microsoft Teams en sus operaciones de Incident Manager mediante la creación de un canal de chat para Microsoft Team en [AWS Chatbot](#) y la adición a continuación de dicho canal en un plan de respuesta.

Para obtener más información, consulte [Uso de los canales de chat en Incident Manager](#).

PagerDuty

[PagerDuty](#) es una herramienta de respuesta a incidentes que admite los flujos de trabajo de paginación y las políticas de escalamiento.

Al integrar Incident Manager con PagerDuty, puede añadir un PagerDuty servicio a su plan de respuesta. Después, se crea el incidente correspondiente en PagerDuty cada vez que se crea un incidente en Incident Manager. El incidente PagerDuty utiliza el flujo de trabajo de paginación y las políticas de escalamiento que usted definió allí, además de las de Incident Manager. PagerDuty adjunta los eventos de la cronología de Incident Manager como notas sobre el incidente.

Para integrar Incident Manager PagerDuty, primero debe crear un identificador secreto AWS Secrets Manager que contenga sus PagerDuty credenciales.

Para obtener información sobre cómo añadir una clave de API PagerDuty REST y otros detalles necesarios a una entrada secreta AWS Secrets Manager, consulte [Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager](#).

Para obtener información sobre cómo agregar un PagerDuty servicio de su PagerDuty cuenta a un plan de respuesta en Incident Manager, consulte los pasos para [integrar un PagerDuty servicio en el plan de respuesta](#) en el tema [Creación de un plan de respuesta](#).

ServiceNow

Con él AWS Service Management Connector, puede integrar Incident Manager con [ServiceNow](#) una plataforma de flujo de trabajo de terceros basada en la nube.

Después de configurar la integración con ServiceNow, al crear un nuevo incidente en Incident Manager, la integración ServiceNow también crea el incidente. Si actualiza un incidente en Incident Manager, este realizará estas actualizaciones en el incidente correspondiente ServiceNow. Si resuelve un incidente en Incident Manager o ServiceNow, la integración resuelve el incidente en ambos servicios en función de las preferencias que configure.

Para obtener más información, consulte [Integración AWS Systems Manager Incident Manager ServiceNow en](#) la Guía AWS Service Management Connector del administrador.

Slack

[Slack](#) proporciona herramientas de colaboración basadas en la nube para mensajería en equipo, audioconferencias y videoconferencias, y uso compartido de archivos.

Puede integrar un canal de Slack en sus operaciones de Incident Manager mediante la creación de un canal de chat para Slack en [AWS Chatbot](#) y la adición a continuación de dicho canal en un plan de respuesta.

Para obtener más información, consulte [Uso de los canales de chat en Incident Manager](#).

Terraform

HashiCorp [Terraform](#) es una herramienta de software de infraestructura como código (IaC) de código abierto que proporciona un flujo de trabajo de interfaz de línea de comandos (CLI) para administrar varios servicios en la nube. En el caso de Incident Manager, puede utilizar Terraform para administrar o aprovisionar lo siguiente:

Recursos de contactos de SSM Incident Manager

- [aws_ssmcontacts_contact](#)
- [aws_ssmcontacts_contact_channel](#)
- [aws_ssmcontacts_plan](#)
- [aws_ssmcontacts_rotation](#)

Fuentes de datos de contactos SSM

- [aws_ssmcontacts_contact](#)
- [aws_ssmcontacts_contact_channel](#)
- [aws_ssmcontacts_plan](#)
- [aws_ssmcontacts_rotation](#)

Recursos de Incident Manager de SSM

- [aws_ssmincidents_replication_set](#)
- [aws_ssmincidents_response_plan](#)

Orígenes de datos de Incident Manager de SSM

- [aws_ssmincidents_replication_set](#)
- [aws_ssmincidents_response_plan](#)

Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager

Tras activar la integración con un plan PagerDuty de respuesta, Incident Manager trabaja con él PagerDuty de las siguientes maneras:

- Incident Manager crea el incidente correspondiente PagerDuty cuando se crea un nuevo incidente en Incident Manager.
- El flujo de trabajo de paginación y las políticas de escalamiento que creó se PagerDuty utilizan en el PagerDuty entorno. Sin embargo, Incident Manager no importa la PagerDuty configuración.
- Incident Manager publica los eventos de la cronología como notas del incidente PagerDuty, con un máximo de 2000 notas.
- Puede optar por resolver automáticamente PagerDuty los incidentes al resolver el incidente relacionado en Incident Manager.

Para integrar Incident Manager con PagerDuty, primero debe crear una entrada secreta AWS Secrets Manager que contenga sus PagerDuty credenciales. Estas permiten a Incident Manager comunicarse con su PagerDuty servicio. A continuación, puede incluir un PagerDuty servicio en los planes de respuesta que cree en Incident Manager.

Este secreto que crea en el Administrador de secretos debe contener, en el formato JSON apropiado, lo siguiente:

- Una clave de API de su PagerDuty cuenta. Puede utilizar una clave API de REST de acceso general o una clave API de REST de token de usuario.
- Una dirección de correo electrónico de usuario válida de tu PagerDuty subdominio.
- La región PagerDuty de servicio en la que implementaste tu subdominio.

Note

Todos los servicios de un PagerDuty subdominio se implementan en la misma región de servicio.

Requisitos previos

Antes de crear el secreto en el Administrador de secretos, asegúrese de satisfacer los siguientes requisitos.

Clave de KMS

Debe cifrar el secreto que cree con una clave gestionada por el cliente que haya creado en AWS Key Management Service (AWS KMS). Debe especificar esta clave al crear el secreto que almacena PagerDuty sus credenciales.

Important

Secrets Manager ofrece la opción de cifrar el secreto con un Clave administrada de AWS, pero este modo de cifrado no es compatible.

La clave administrada por el cliente debe cumplir los siguientes requisitos:

- Tipo de clave: elija Simétrica.
- Uso de la clave: elija Cifrado y descifrado.
- Regionalidad: si desea replicar su plan de respuesta en varias Regiones de AWS, asegúrese de seleccionar la clave multirregional.

Política de claves

El usuario que configure el plan de respuesta debe tener permiso para `kms:GenerateDataKey` y `kms:Decrypt` en la política basada en recursos de la clave. La entidad principal del servicio `ssm-incidents.amazonaws.com` debe tener permiso para `kms:GenerateDataKey` y `kms:Decrypt` en la política basada en recursos de la clave.

La siguiente política demuestra estos permisos. Reemplace cada *marcador de posición de entrada del usuario* con información propia.

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "Enable IAM user permissions",
      "Effect": "Allow",
```

```

    "Principal": {
      "AWS": "arn:aws:iam::account-id:root"
    },
    "Action": "kms:*",
    "Resource": "*"
  },
  {
    "Sid": "Allow creator of response plan to use the key",
    "Effect": "Allow",
    "Principal": {
      "AWS": "IAM_ARN_of_principal_creating_response_plan"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey*"
    ],
    "Resource": "*"
  },
  {
    "Sid": "Allow Incident Manager to use the key",
    "Effect": "Allow",
    "Principal": {
      "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey*"
    ],
    "Resource": "*"
  }
]
}

```

Para obtener información sobre la creación de una nueva clave administrada por el cliente, consulte [Creación de claves de KMS de cifrado simétricas](#) en la Guía para desarrolladores de AWS Key Management Service . [Para obtener más información sobre AWS KMS las claves, consulte AWS KMS los conceptos.](#)

Si una clave administrada por el cliente existente cumple todos los requisitos anteriores, puede editar su política para añadir estos permisos. Para obtener información sobre la actualización de la política de una clave administrada por el cliente, consulte [Modificación de una política de clave](#) en la Guía para desarrolladores de AWS Key Management Service .

i Tip

Puede especificar una clave de condición para limitar aún más el acceso. Por ejemplo, la siguiente política permite el acceso a través del Administrador de secretos solo en la región este de EE. UU. (Ohio) (us-east-2):

```
{
  "Sid": "Enable IM Permissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "ssm-incidents.amazonaws.com"
  },
  "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
    }
  }
}
```

Permiso **GetSecretValue**

La identidad de IAM (usuario, rol o grupo) que crea el plan de respuesta debe tener el permiso de IAM `secretsmanager:GetSecretValue`.

Para almacenar las credenciales de PagerDuty acceso en AWS Secrets Manager secreto

1. Siga los pasos del paso 3a de la sección [Crear un AWS Secrets Manager secreto](#) de la Guía del AWS Secrets Manager usuario.
2. En el paso 3b, en Pares clave/valor, haga lo siguiente:
 - Elija la pestaña Texto sin formato.
 - Sustituya el contenido predeterminado del cuadro por la siguiente estructura JSON:

```
{
  "pagerDutyToken": "pagerduty-token",
  "pagerDutyServiceRegion": "pagerduty-region",
  "pagerDutyFromEmail": "pagerduty-email"
}
```

```
}
```

- En el ejemplo JSON que ha pegado, sustituya los *valores de marcador de posición* por los siguientes:

- *pagerduty-token*: el valor de una clave de API REST de acceso general o de una clave de API REST de token de usuario de tu cuenta. PagerDuty

Para obtener información relacionada, consulte las [claves de acceso a las API](#) en la base de conocimientos. PagerDuty

- *pagerduty-region*: *la región* de servicio del centro de PagerDuty datos que aloja su subdominio. PagerDuty

Para obtener información relacionada, consulte las [regiones de servicio](#) en la base de conocimientos. PagerDuty

- *pagerduty-email*: la dirección de correo electrónico válida de un usuario que pertenece a tu subdominio. PagerDuty

Para obtener información relacionada, consulte [Administrar usuarios](#) en la base de conocimientos. PagerDuty

El siguiente ejemplo muestra un secreto JSON completado que contiene las PagerDuty credenciales necesarias:

```
{
  "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
  "pagerDutyServiceRegion": "US",
  "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. En el paso 3c, en Clave de cifrado, elija una clave administrada por el cliente que haya creado y que cumpla los requisitos enumerados en la sección Requisitos previos anterior.
4. En el paso 4c, en Permisos de recursos, haga lo siguiente:
 - Expanda Permisos de recursos.
 - Elija Editar permisos.
 - Sustituya el contenido predeterminado del cuadro de políticas por la siguiente estructura JSON:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "ssm-incidents.amazonaws.com"
  },
  "Action": "secretsmanager:GetSecretValue",
  "Resource": "*"
}
```

- Elija Guardar.
5. En el paso 4d, en Replicar secreto, haga lo siguiente si ha replicado su plan de respuesta a más de una Región de AWS:
 - Expanda Replicar secreto.
 - En Región de AWS, seleccione la región a la que replicó su plan de respuesta.
 - En Clave de cifrado, elija una clave administrada por el cliente que haya creado en esta región o haya replicado a la misma y que cumpla los requisitos enumerados en la sección Requisitos previos.
 - Para cada uno de los adicionales Región de AWS, elige Añadir región y selecciona el nombre de la región y la clave gestionada por el cliente.
 6. Complete los pasos restantes de [Crear un AWS Secrets Manager secreto](#) en la Guía del AWS Secrets Manager usuario.

Para obtener información sobre cómo agregar un PagerDuty servicio al flujo de trabajo de incidentes de Incident Manager, consulte [Integrar un PagerDuty servicio en el plan de respuesta](#) en el tema [Creación de un plan de respuesta](#).

Información relacionada

[Cómo automatizar la respuesta a los incidentes con PagerDuty y AWS Systems Manager Incident Manager](#) (blog sobre Nube de AWS operaciones y migraciones)

[Cifrado de secretos en AWS Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager

Solución de problemas de AWS Systems Manager Incident Manager

Si encuentra algún problema al utilizar AWS Systems Manager Incident Manager, puede utilizar la siguiente información para resolverlos de acuerdo con nuestras prácticas recomendadas. Si cualquier problema que encontrase estuviera fuera del ámbito de la siguiente información, o si persistiera después de haber intentado resolverlo, póngase en contacto con [AWS Support](#).

Temas

- [Mensaje de error: ValidationException – We were unable to validate the AWS Secrets Manager secret](#)
- [Otras incidencias en la solución de problemas](#)

Mensaje de error: **ValidationException – We were unable to validate the AWS Secrets Manager secret**

Problema 1: La identidad de AWS Identity and Access Management (IAM) (usuario, rol o grupo) que crea el plan de respuesta no tiene el permiso de IAM `secretsmanager:GetSecretValue`. Las identidades de IAM deben tener este permiso para validar los secretos del administrador de secretos.

- Solución: Añada el permiso `secretsmanager:GetSecretValue` que falta a la política de IAM para la identidad de IAM que crea el plan de respuesta. Para obtener más información, consulte [Adición de permisos de identidad de IAM \(consola\)](#) o [Adición de políticas de IAM \(AWS CLI\)](#) en la Guía del usuario de IAM.

Problema 2: El secreto no tiene vinculada una política basada en recursos que permita a la identidad de IAM ejecutar la acción [GetSecretValue](#) o la política basada en recursos deniega el permiso a la identidad.

- Solución: Cree o añada una declaración Allow a la política basada en recursos del secreto que conceda permiso para `secrets:GetSecretValue` a la identidad de IAM. O bien, si utiliza una declaración Deny que incluya la identidad de IAM, actualice la política para que la identidad pueda ejecutar la acción. Para obtener más información, consulte [Adición de una política de permisos a un secreto de AWS Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager.

Problema 3: Los secretos no tienen vinculada una política basada en recursos que permita el acceso a la entidad principal del servicio de Incident Manager `ssm-incidents.amazonaws.com`.

- Solución: Cree o actualice la política basada en recursos para el secreto e incluya el siguiente permiso:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": ["ssm-incidents.amazonaws.com"]
  },
  "Action": "secretsmanager:GetSecretValue",
  "Resource": "*"
}
```

Problema 4: El AWS KMS key seleccionado para cifrar el secreto no es una clave administrada por el cliente, o la clave administrada por el cliente seleccionada no proporciona los permisos de IAM `kms:Decrypt` y `kms:GenerateDataKey*` a la entidad principal del servicio de Incident Manager. Asimismo, la identidad de IAM que crea el plan de respuesta podría no tener el permiso de IAM [GetSecretValue](#).

- Solución: Asegúrese de satisfacer los requisitos descritos en Requisitos previos que figuran en el tema [Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager](#).

Problema 5: El ID del secreto que contiene la clave de la API de REST de acceso general o la clave de la API de REST del token de usuario no es válido.

- Solución: Asegúrese de haber introducido el ID del secreto del administrador de secretos con precisión, sin espacios al final. Debe trabajar en el mismo Región de AWS que almacena el secreto que desea utilizar. No puede utilizar un secreto eliminado.

Problema 6: En raras ocasiones, el servicio de Incident Manager podría experimentar algún problema, o Incident Manager podría tener problemas para comunicarse con el mismo.

- Solución: Espere unos minutos y vuelva a intentarlo. Compruebe en [AWS Health Dashboard](#) cualquier problema que pudiera afectar a cualquiera de los dos servicios.

Otras incidencias en la solución de problemas

Si los pasos anteriores no resolvieron su problema, puede encontrar ayuda adicional en los siguientes recursos:

- Para cuestiones de IAM específicas de Incident Manager al acceder a la [consola de Incident Manager](#), consulte [Solución de problemas AWS Systems Manager Incident Manager de identidad y acceso](#).
- Para problemas generales de autenticación y autorización al acceder a la AWS Management Consoleconsola de IAM, [consulte](#) Solución de problemas de IAM en la Guía del usuario de IAM.

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el [Glosario de AWS](#) en la Referencia de Glosario de AWS.

Historial de documentos de Incident Manager

Cambio	Descripción	Fecha
Actualización de la política gestionada AWS Incident Manager IncidentAccessServiceRolePolicy	Incident Manager ha agregado un nuevo permiso <code>AWSIncidentManagerIncidentAccessServiceRolePolicy</code> , en apoyo de la función Findings, que le permite comprobar si una instancia EC2 forma parte de un grupo de Auto Scaling. Para obtener más información, consulte las actualizaciones de Incident Manager a las políticas AWS gestionadas .	20 de febrero de 2024
Soporte adicional de HashiCorp Terraform: rotaciones de guardia	Terraform ha ampliado su soporte para Incident Manager. Ahora puede aprovisionar o gestionar los recursos disponibles de Incident Manager con Terraform. Para obtener información sobre esta y otras integraciones de terceros con Incident Manager, consulte Integración con otros productos y servicios.	2 de febrero de 2024
Nueva función: Hallazgos de otros Servicios de AWS	Los resultados le proporcionan información sobre los cambios relacionados con las AWS CloudFormation pilas y AWS CodeDeploy las	15 de noviembre de 2023

implementaciones que se produjeron aproximadamente al mismo tiempo que se creó un incidente en Incident Manager. En la consola de Incident Manager, puede ver información resumida sobre esos cambios y, en muchos casos, acceder a los enlaces a la CloudFormation o a las CodeDeploy consolas para obtener información completa sobre el cambio. Los resultados reducen el tiempo necesario para evaluar las posibles causas de los incidentes. También reducen la probabilidad de que los respondedores accedan a la cuenta o consola equivocada para investigar la causa de un incidente. Esta función también introduce una nueva política gestionada AWS IncidentManagerIncidentAccessServiceRolePolicy, que permite a Incident Manager leer los recursos de otras fuentes Servicios de AWS para identificar los hallazgos relacionados con los incidentes. Para obtener más información, consulte los temas siguientes:

- [Uso de los resultados](#)

- [AWS política gestionada: AWSIncidentManagerIncidentAccessServiceRolePolicy](#)

[Listas actualizadas de integraciones con Incident Manager](#)

El tema [Integraciones de productos y servicios con Incident Manager](#) se ha ampliado a fin de enumerar y describir todas las herramientas de Servicios de AWS y de terceros que puede integrar con Incident Manager en sus operaciones de detección y respuesta a incidentes.

9 de junio de 2023

[Integración con AWS Trusted Advisor](#)

28 de abril de 2023

Trusted Advisor ahora comprueba que la configuración de un conjunto de replicación utilice más de uno Región de AWS para admitir la conmutación por error y la respuesta regionales. Para los incidentes creados por CloudWatch alarmas o EventBridge eventos, Incident Manager crea un incidente al Región de AWS igual que la regla de alarma o evento. Si Incident Manager no está disponible temporalmente en esa región, el sistema intenta crear un incidente en otra región dentro del conjunto de replicación. Si el conjunto de replicación incluye solo una región, el sistema no podrá crear un registro de incidentes mientras Incident Manager no esté disponible. Para evitar esta situación, Trusted Advisor informa cuando un conjunto de replicación está configurado para una sola región. Para obtener información sobre el uso de Trusted Advisor, consulte [AWS Trusted Advisor](#) en la Guía del usuario de AWS Support .

[Uso de Microsoft Teams como canal de chat en los planes de respuesta](#)

Gracias a la integración con Microsoft Teams AWS Chatbot, ahora puedes usar Microsoft Teams para el canal de chat en tus planes de respuesta. Esto se suma a la compatibilidad con los canales de chat de Slack y Amazon Chime. Durante un incidente, Incident Manager envía notificaciones de estado directamente a un canal de chat para mantener informados a todos los respondedores. Los socorristas también pueden comunicarse entre sí y con los AWS CLI comandos relacionados con los incidentes en la aplicación Microsoft Teams para actualizar los incidentes e interactuar con ellos. Para obtener más información, consulte [Uso de los canales de chat en Incident Manager](#).

4 de abril de 2023

Nueva característica: Horarios de guardia

Un horario de guardia en Incident Manager define a quién se notifica al producirse un incidente que requiera la intervención de un operario. Un horario de guardia consta de una o más rotaciones que usted crea para el horario. Cada rotación puede incluir hasta 30 contactos. Después de crear un horario de guardia, puede incluirlo como una escalada en su plan de escalada. Al producirse un incidente asociado a ese plan de escalada, Incident Manager lo notifica al operador (u operadores) de guardia según el horario. Para obtener más información, consulte [Uso de los horarios de guardia en Incident Manager](#).

28 de marzo de 2023

[Impresión de un análisis de incidentes formateado o guardado como PDF](#)

La página de análisis de incidentes ahora incluye un botón Imprimir para generar una versión del análisis en formato de impresión. A través de los destinos de impresión configurados para su dispositivo, puede guardar el análisis del incidente como archivo PDF o enviarlo a una impresora local o de red. Para obtener más información, consulte [Impresión de un análisis de incidentes formateado](#).

17 de enero de 2023

[PagerDuty integración: Incident Manager ahora copia los eventos de la cronología de los incidentes en incidentes PagerDuty](#)

Al activar la integración con un plan PagerDuty de respuesta, Incident Manager añade los eventos cronológicos creados a partir de ese plan al registro de incidentes correspondiente PagerDuty. PagerDuty añade los eventos de la cronología como notas sobre el incidente, hasta un máximo de 2000 notas. Para obtener más información sobre estos cambios, consulte los siguientes temas:

15 de diciembre de 2022

- [Guarde las credenciales de PagerDuty acceso en AWS Secrets Manager secreto](#)
- [Integre un PagerDuty servicio en el plan de respuesta](#)

[Integración de Incident Manager con CloudWatch métricas.](#)

Ahora puede publicar las métricas relacionadas con los incidentes en CloudWatch. [Para obtener más información, consulta CloudWatch las métricas.](#) Se [AWSIncidentManagerServiceRolePolicy](#) ha incluido un permiso adicional que permite a nuestro servicio publicar métricas en tu nombre.

15 de diciembre de 2022

[Lanzamiento de Notas del incidente y actualización de la pantalla Detalles del incidente](#)

Con Notas del incidente, puede colaborar y comunicar con otros usuarios que trabajen en un incidente . Además, puede ver los manuales de procedimientos y los estados de participación desde la pantalla Detalles del incidente. Para obtener más información, consulte [Detalles del incidente](#).

16 de noviembre de 2022

[Integre los planes de PagerDuty escalamiento y los flujos de trabajo de localización en los planes de respuesta de Incident Manager](#)

Ahora puede integrar Incident Manager PagerDuty y añadir un PagerDuty servicio a un plan de respuesta. Tras configurar la integración, Incident Manager puede crear un incidente correspondiente PagerDuty para cada nuevo incidente creado en Incident Manager. PagerDuty utiliza el flujo de trabajo de paginación y las políticas de escalamiento que usted define en el PagerDuty entorno.

16 de noviembre de 2022

Para obtener más información, consulte los temas siguientes:

- [Integraciones de productos y servicios con Incident Manager](#)
- [Guarde las credenciales de PagerDuty acceso en secreto AWS Secrets Manager](#)
- [Integre un PagerDuty servicio en el plan de respuesta del tema \[Creación de un plan de respuesta\]\(#\)](#)
- [Solución de problemas](#)

[Lanzamiento de Notas del incidente y actualización de la pantalla Detalles del incidente.](#)

Con Notas del incidente, puede colaborar y comunicar con otros usuarios que trabajen en un incidente . Además, puede ver los manuales de procedimientos y los estados de participación desde la pantalla Detalles del incidente. Para obtener más información, consulte [Detalles del incidente](#).

16 de noviembre de 2022

[Soporte de etiquetado para conjuntos de réplica](#)

Ahora puede asignar etiquetas a su conjunto de réplica en AWS Systems Manager Incident Manager. Esto se suma al soporte existente para asignar etiquetas a los planes de respuesta, los registros de incidentes y los contactos Regiones de AWS especificados en el conjunto de replicación. Para obtener información, consulte los siguientes temas:

2 de noviembre de 2022

- [Asistente de preparación](#)
- [Etiquetado de recursos en Incident Manager](#)

[Integración de Incident Manager con Atlassian Jira Service Management](#)

Puedes integrar Incident Manager con [Jira Service Management](#) mediante el conector de administración de servicios para Jira AWS Service Management. Después de configurar la integración, los nuevos incidentes creados en Incident Manager crean un incidente correspondiente en Jira. Al actualizar un incidente en Incident Manager, las actualizaciones se añaden al incidente correspondiente en Jira. Si resuelve un incidente en Incident Manager o en Jira, también se resuelve el incidente correspondiente, según las preferencias configuradas. Para obtener más información, consulte [Configuración de Jira Service Management](#) en la Guía del administrador del conector de administración de servicios de AWS .

6 de octubre de 2022

[Soporte de etiquetado mejorado](#)

Incident Manager permite asignar etiquetas a los planes de respuesta, los registros de incidentes y los contactos Regionales de AWS especificados en el conjunto de réplicas. Incident Manager también admite la asignación automática de etiquetas a incidentes creados a partir de planes de respuesta. Para obtener más información, consulte [Etiquetado de recursos de Incident Manager](#).

28 de junio de 2022

[Integración de Incident Manager con ServiceNow](#)

9 de junio de 2022

Puede integrar Incident Manager [ServiceNow](#) mediante el conector de administración de AWS servicios para ServiceNow. Tras configurar la integración, los nuevos incidentes creados en Incident Manager crean el incidente correspondiente en ServiceNow. Si actualiza un incidente en Incident Manager, las actualizaciones se añaden al incidente correspondiente en ServiceNow. Si resuelve un incidente en el Administrador de incidentes o ServiceNow, el incidente correspondiente también se resuelve, según las preferencias configuradas. Para obtener más información, consulte [Integrar AWS Systems Manager Incident Manager en ServiceNow](#).

[Importación de datos de contacto](#)

Al crearse un incidente, Incident Manager puede avisar a los respondedores mediante notificaciones de voz o SMS. Para garantizar que los respondedores vean que la llamada o la notificación por SMS procede de Incident Manager, recomendamos que todos los respondedores descarguen el archivo formato de tarjeta virtual (.vcf) de Incident Manager a la libreta de direcciones de sus dispositivos móviles. Para obtener más información, consulte [Importación de datos de contacto a su libreta de direcciones](#).

18 de mayo de 2022

[Múltiples mejoras de características para mejorar la creación y corrección de incidentes](#)

17 de mayo de 2022

Incident Manager lanzó las siguientes mejoras de características para mejorar la creación y corrección de incidentes:

- Crear incidentes automáticamente en otras Regiones de AWS: en el caso de que Incident Manager no esté disponible en una Región de AWS cuando Amazon CloudWatch o Amazon EventBridge creen un incidente, estos servicios ahora crean automáticamente el incidente en una de las regiones disponibles especificadas en su conjunto de replicaciones. Para obtener más información, consulte [Administración de incidentes entre regiones](#).
- Rellene automáticamente los parámetros del manual con los metadatos de los incidentes: ahora puede configurar Incident Manager para recopilar información sobre los recursos de AWS derivados de los incidentes. Incident Manager puede entonces rellenar los parámetros del manual de procedimientos con la

información recopilada.

Para obtener más información, consulte [Tutorial: Uso de manuales de procedimientos de automatización de Systems Manager con Incident Manager](#).

- Recopile automáticamente la información sobre los AWS recursos: cuando el sistema crea un incidente , Incident Manager ahora recopila automáticamente información sobre los AWS recursos involucrados en el incidente. A continuación, Incident Manager añade esta información a la pestaña Elementos relacionados.

[Admisión de múltiples manuales de procedimientos](#)

Incident Manager ahora admite la ejecución de varios manuales de procedimientos durante un incidente para la página de detalles del incidente.

14 de enero de 2022

[Incident Manager se lanzó en una nueva versión Regiones de AWS](#)

Incident Manager ya está disponible en estas nuevas regiones: us-west-1, sa-east-1, ap-northeast-2, ap-south-1, ca-central-1, eu-west-2 y eu-west-3. Para obtener más información sobre regiones y cuotas de Incident Manager, consulte la [Guía de referencia de Referencia general de AWS](#).

8 de noviembre de 2021

[Reconocimiento de participación en la consola](#)

Ahora puede reconocer las participaciones directamente desde la consola de Incident Manager.

5 de agosto de 2021

[Pestaña Propiedades](#)

Incident Manager introdujo una pestaña de propiedad es en la página de detalles del incidente, que proporciona más información sobre los incidentes OpsItem, su origen y el análisis posterior al incidente.

3 de agosto de 2021

[Lanzamiento de Incident Manager](#)

Incident Manager es una consola de gestión de incidentes diseñada para ayudar a los usuarios a mitigar los incidentes que afectan a sus aplicaciones AWS alojadas y a recuperarse de ellos.

10 de mayo de 2021

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.